Scarlet Box

Manuel d'installation

Basé sur le *firmware* 6.0

Traduction officieuse réalisée par Jacques Theys
farenheid@scarlet.be

Historique du document :

Date	Version	Statut	Description
6 avril 2005	1.0Scarlet-FR	Essai	Premier jet de la traduction basé sur le manuel CopperJet 816-2P

Légal

Ce document est une traduction totalement officieuse basée sur le manuel du CopperJet 816-2P d'Allied Data Technologies. Le produit décrit dans ce document, la Scarlet Box, est un appareil fournit par la société Scarlet à ses clients ayant souscrit la formule Scarlet One. Bien que les deux appareils soient similaires, des différences peuvent apparaître.

Plusieurs éléments du manuel original décrivant le CopperJet 816-2P ont été adaptés afin de correspondre à l'utilisation d'une Scarlet Box sur le réseau Scarlet. Les captures d'écran ont été réalisées sous FireFox 1.0.2 sur base des écrans présentés par une Scarlet Box nantie du *firmware* Scarlet One 6.00 SR4C. Il se peut que ces écrans diffèrent des écrans de votre Scarlet Box.

Je (Jacques Theys) n'assume aucune responsabilité quant à l'exactitude des informations fournies dans ce document. Il ne s'agit que d'un travail fourni à titre gracieux pour aider la communauté des utilisateurs de Scarlet One dans la configuration et l'utilisation de leur Scarlet Box.

Ni Scarlet, ni Belgacom, ni Allied Data Technologies ne sont en aucun cas responsables des informations fournies dans ce document.

Pour les dispositions légales du manuel original, veuillez vous référer à l'adresse suivante : ftp://ftp.allieddata.com/public/Product_Info/xDSL_Products/CopperJet_816_2P/Firmware_6.x/Manuals/Installation_Manual_CJT_816_2Pv1.0.pdf

Pour m'écrire : farenheid@scarlet.be

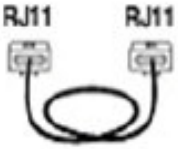
Légal 3
1. Contenu de la boîte 6
2. Témoins lumineux avant et panneau arrière 7
2.1. Témoins lumineux de la Scarlet Box 7
2.2. Panneau arrière de la Scarlet Box 7
3. Installation de la Scarlet Box 8
3.1. Connexion de la Scarlet Box 8
4. Avant de commencer 10
4.1. Nom d'utilisateur et mot de passe 10
4.2. Adresses des serveurs DNS, de courrier, newsgroups et proxy 10
5. Configurer la Scarlet Box 11
5.1. Accéder au serveur web intégré 11
5.2. Démarrage rapide - QuickStart 12
5.3. Options du système - System 13
5.3.1. Journal d'activité - Event Log 13
5.3.2. Informations sur l'appareil - Device Info 13
5.3.3. Accès distant - Remote Access 14
5.3.4. Mise à jour du logiciel système 16
5.3.5. Sauvegarde du profil de configuration 16
5.3.6. Redémarrage de l'appareil – Restart Device 17
5.4. Configuration 18
5.4.1. Sauvegarde de la configuration – Save Config 18
5.4.2. Se connecter au serveur web intégré 18
5.4.3. Modifier les paramètres de connexion – Authentication 18
5.5. Connexions réseau – LAN Connection 20
5.5.1. Editer une connexion réseau – Edit a LAN connection 20
5.6. Connexions externes – WAN Connections 23
5.6.1. Configurer une connexion RFC1483 Bridged 24
5.6.1.1. Configurer DHCP pour votre carte réseau 25
5.6.2. Configurer une connexion RFC1483 Routed 26
5.6.3. Configurer une connexion PPPoA Routed 28
5.6.4. Configurer une connexion PPPoE Routed 30
5.7. Sécurité – Security 32
5.7.1. Activation de la sécurité 33
5.7.2. Configuration des interfaces sécurisées 33
5.7.3. Configuration de la translation d'adresses (NAT) 34
5.7.3.1. Réserver des affectations dans la translation d'adresses 35
5.7.4. Activation du pare-feu (*firewall*) 37
5.7.5. Activer la détection d'intrusions 37
5.7.6. Configuration des *triggers* 37
5.7.6.1. Ajouter un *trigger* 38
5.7.6.2. Supprimer un *trigger* 39
5.8. Chercher un service – Search Service 39
5.9. Pont PPP sans installation – Zero Installation PPP Bridge (ZIPB) 41
5.9.1. ZIPB dans les configuration utilisant un pont 41
5.9.2. ZIPB dans les configuration utilisant une translation d'adresses 41
5.9.3. Activer/désactiver ZIPB 41
5.9.4. Configuration avancée de ZIPB – ZIPB Advanced configuration 42
5.9.5. Limitations de ZIPB 44
5.10. Routes IP – IP Routes 44
5.10.1. Créer une route IPv4 44
5.11. Serveur DHCP – DHCP Server 46
5.11.1. Configurer un serveur DHCP 46
5.11.2. Créer un hôte fixe – Create fixed host 48

5.11.3. Désactiver le serveur DHCP 49
5.12. Configurer le client DNS 50
5.12.1. Configurer des serveurs DNS 50
5.12.2. Configurer les domaines DNS à explorer 50
5.13. Configurer le relais DNS 50
5.13.1. Configurer manuellement le relais DNS 51
5.13.2. Découvrir automatiquement les adresses DNS relais 51
5.13.3. Configurer la base de données DNS du réseau local 52
5.14. Configurer le service Voix sur DSL – Voice over DSL 53
5.14.1. Paramètres de base du service Voix sur DSL 53
5.15. Ligne DSL – DSL Line 55
5.16. Ethernet 57

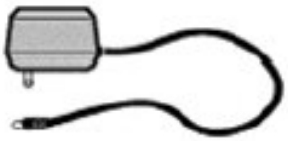
1. Contenu de la boîte

Votre boîte devrait contenir les éléments suivants :

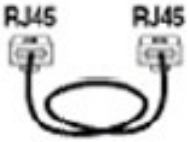
Scarlet Box



2 câbles téléphoniques



Adaptateur secteur



Câble Ethernet RJ-45 croisé

Filtre ACS

Filtre ADSL

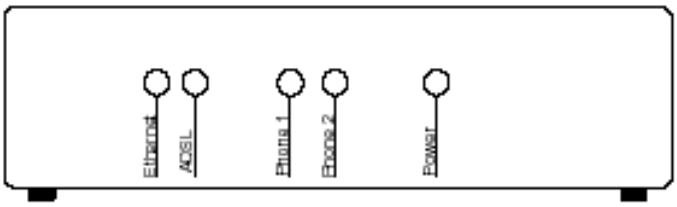
ATTENTION : pour éviter toute surchauffe, assurez-vous que la Scarlet Box dispose d'espace libre autour d'elle afin de permettre la circulation de l'air.

2. Témoins lumineux avant et panneau arrière

Avant de commencer l'installation, prenez un moment pour vous familiariser avec les témoins lumineux avant et le panneau arrière de votre Scarlet Box.

2.1. Témoins lumineux de la Scarlet Box

Panneau avant



Ethernet : le témoin « Ethernet » s'allume lorsque vous connectez votre Scarlet Box à un port Ethernet sur votre ordinateur ou sur un *hub*/*switch*.

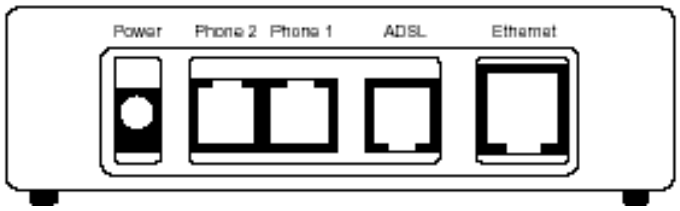
ADSL : le témoin « ADSL » clignote lorsque la négociation des protocoles DSL débute. Il reste allumé en continu lorsque le réseau ADSL est correctement configuré et connecté.

Phone : les témoins « Phone » clignotent quand le téléphone connecté reçoit un appel entrant. Lors d'une connexion par modem analogique, le clignotement indique que la suppression de l'écho est désactivée. Le témoin « Phone » est allumé en continu lorsque le combiné téléphonique est décroché.

Power : le témoin « Power » est allumé quand la Scarlet Box est connectée à une source d'alimentation électrique.

2.2. Panneau arrière de la Scarlet Box

Panneau arrière



Power : seul l'adaptateur fourni peut être connecté à la prise Power.

Phone : pour connecter votre téléphone analogique à la Scarlet Box.

ADSL : pour connecter votre Scarlet Box sur la ligne ADSL de Scarlet.

Ethernet : pour connecter votre Scarlet Box sur votre ordinateur, un *hub* ou un *switch*.

3. Installation de la Scarlet Box

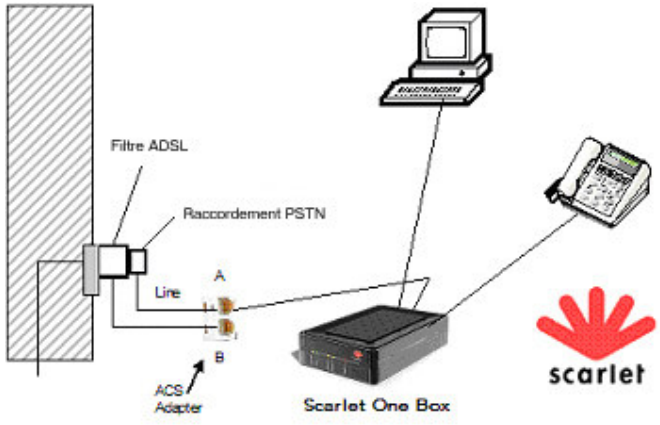
Pour connecter votre Scarlet Box à votre ordinateur, ce dernier doit disposer d'une carte Ethernet 10/100Base-T (la plupart des ordinateurs récents en possèdent).

Si vous utilisez des adresses IP statiques, vous devez posséder une adresse IP qui se situe dans le même sous-réseau que l'interface web de votre Scarlet Box. L'adresse IP par défaut de l'interface est 172.19.3.1. Si vous utilisez les adresses IP par défaut, votre carte réseau peut avoir l'adresse IP 172.19.3.2 avec le masque de sous-réseau 255.255.0.0. Utilisez l'adresse 172.19.3.1 comme passerelle.

Vous pouvez également configurer votre carte réseau pour obtenir automatiquement une adresse IP et laisser le serveur DHCP de la Scarlet Box la configurer pour vous.

3.1. Connexion de la Scarlet Box

La connexion de la Scarlet Box se fait dans un premier temps selon le schéma suivant :

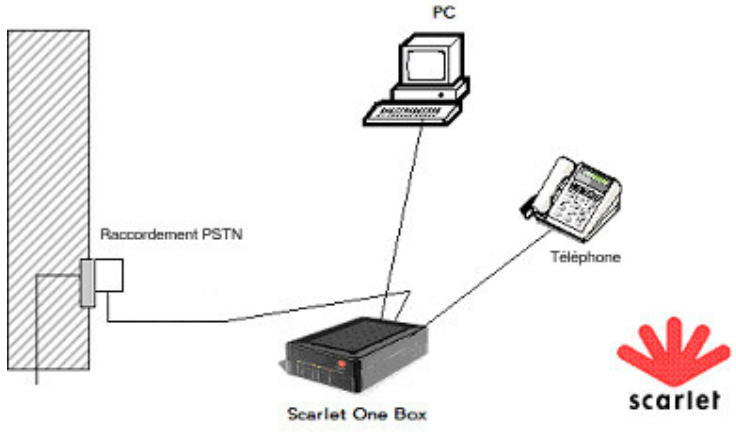


Connectez le filtre ACS à la prise ADSL de votre Scarlet Box.
Branchez le filtre ADSL dans la prise téléphonique murale à cinq pôles. Insérez un câble téléphonique dans la prise ADSL du filtre et dans la prise B du filtre ACS.
Connectez le deuxième câble téléphonique à la prise A du filtre ACS à l'aide d'une prise téléphonique 5 pôles insérée dans la partie téléphone du filtre ADSL.
Assurez-vous de brancher les deux câbles téléphoniques sur les prises adéquates du filtre ACS. Un raccordement inverse **ne fonctionne pas**. Le câble reliant la partie ADSL du filtre ADSL et le filtre ACS ne peut dépasser 5 mètres.

Insérez le câble Ethernet dans la prise Ethernet de votre Scarlet Box. Branchez l'autre extrémité à la prise Ethernet 10/100Base-T de votre PC ou sur votre *hub*/*switch*.
Si vous connectez votre Scarlet Box sur un *hub* ou un *switch*, il se peut que vous ayez à utiliser un câble Ethernet droit au lieu du câble croisé fourni.

Cette configuration vous permet de profiter de l'ADSL et de téléphoner gratuitement via le réseau Scarlet en attendant le portage définitif de votre numéro. Vos appels entrants sont toujours pris en charge par Belgacom.

Lorsque Scarlet vous avertit que votre numéro de téléphone a été porté entièrement vers son réseau, vous pouvez éliminer le filtre ACS de votre installation et ne conserver qu'un seul câble téléphonique raccordé sur la prise ADSL de votre filtre ADSL et sur la prise ADSL de votre Scarlet Box selon le schéma suivant :



Le filtre ADSL peut, dans de nombreux cas, être éliminé également.

Les informations de connexion officielles de Scarlet sont disponibles aux adresses suivantes :

- Pour connecter un téléphone :
  http://www.scarlet.be/fr/assistance/scarlet_one/scarlet_box/a147558

- Pour connecter plusieurs téléphones :
  http://www.scarlet.be/fr/assistance/scarlet_one/scarlet_box/a147560

4. Avant de commencer

Les informations suivantes vous seront utiles lorsque vous configurerez votre Scarlet Box. Assurez-vous d'en disposer avant de commencer la configuration de la Scarlet Box.

4.1. Nom d'utilisateur et mot de passe

Votre nom d'utilisateur (*login*) et votre mot de passe vous ont été fournis par Scarlet.

4.2. Adresses des serveurs DNS, de courrier, newsgroups et proxy

Ces adresses ne sont pas strictement nécessaires à la configuration de votre Scarlet Box mais peuvent vous être utiles quand vous configurerez votre ordinateur.

Les adresses des DNS de Scarlet sont automatiquement attribués lorsque vous vous connectez au réseau Scarlet.
Si vous avez besoin des adresses des serveurs Scarlet (DNS, courrier, *newsgroups*, *proxy*), vous pouvez les trouver à l'adresse http://www.scarlet.be/fr/assistance/.

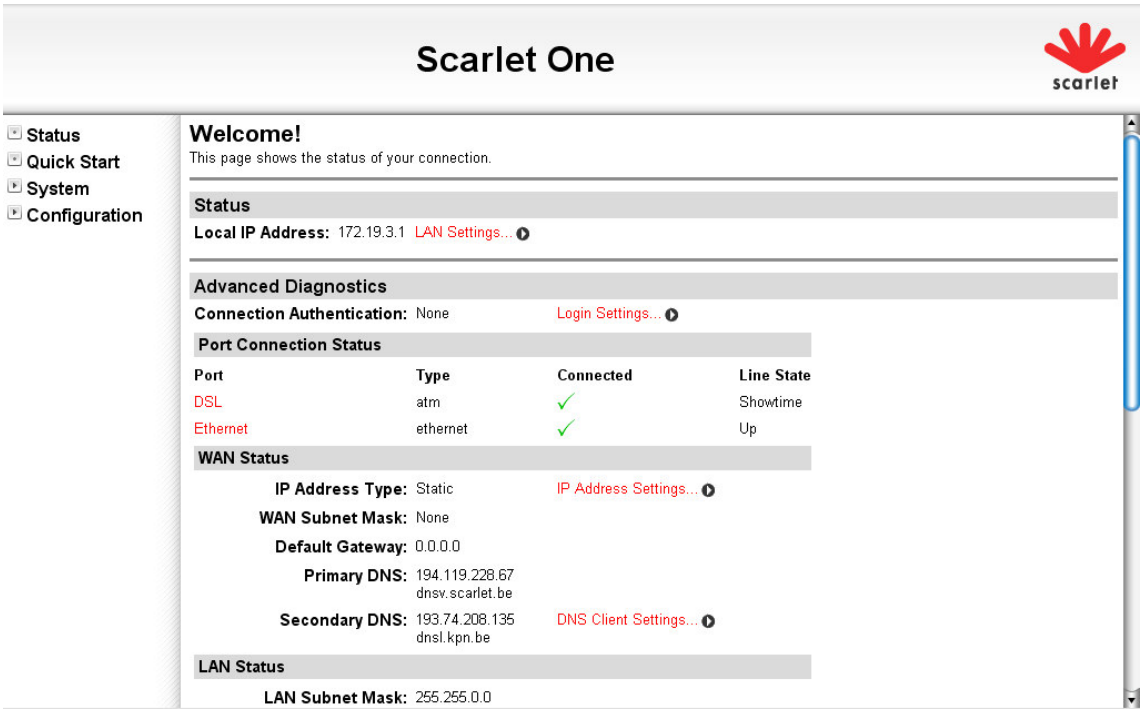
5. Configurer la Scarlet Box

La configuration de la Scarlet Box est effectuée via le serveur http web intégré. Vous pouvez y accéder à l'aide d'un navigateur standard tel que Microsoft Internet Explorer, Netscape Navigator ou FireFox.

5.1. Accéder au serveur web intégré

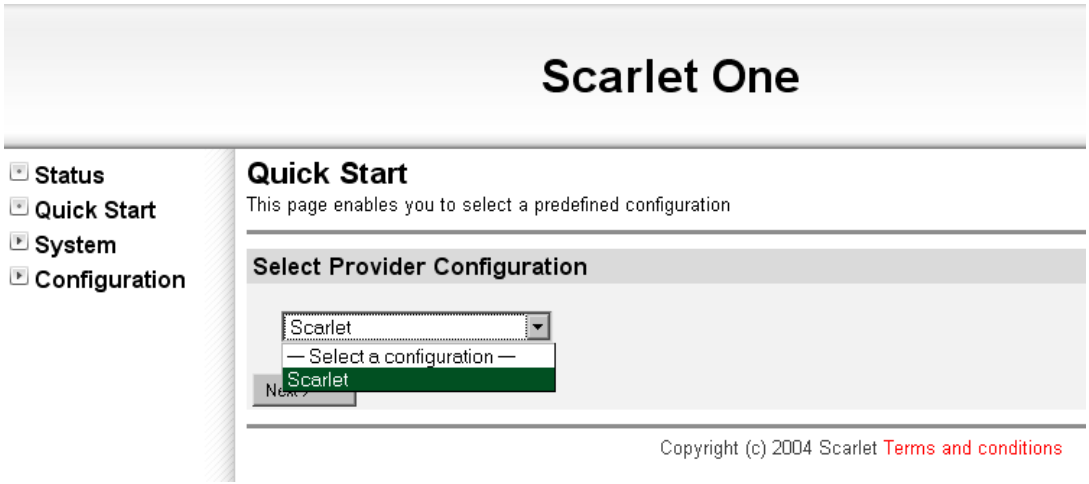
Pour accéder au serveur web intégré, lancez votre navigateur et entrez l'adresse IP de la Scarlet Box dans la barre d'adresse. L'adresse IP par défaut de la Scarlet Box est 172.19.3.1. Donc, l'adresse à entrer dans la barre est http://172.19.3.1.

Lors du premier accès au serveur web intégré, un message de bienvenue *Welcome !* vous est présenté. Il est replacé par une entête *Status* lorsque la page est automatiquement ou manuellement rechargée:



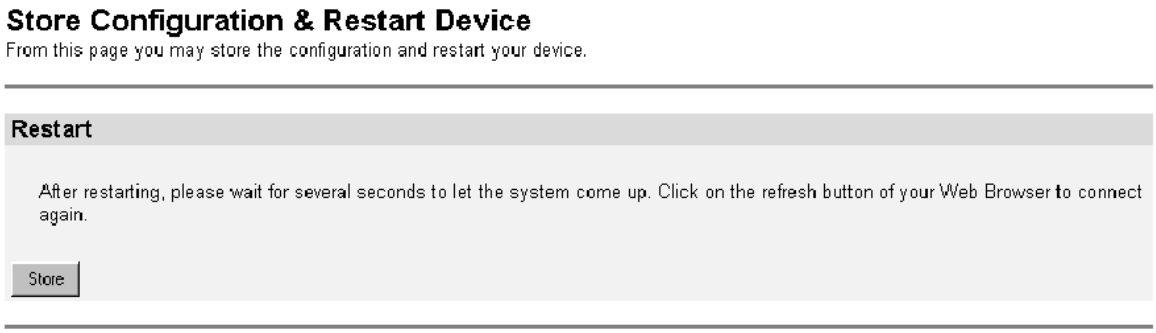
5.2. Démarrage rapide – QuickStart

Grâce à l'option *QuickStart* (démarrage rapide), vous pouvez configurer votre Scarlet Box en quelques étapes.
Pour utiliser *QuickStart*, cliquez sur *QuickStart* dans la colonne de gauche. La page *QuickStart* s'affiche alors. Sélectionnez Scarlet dans la liste *Select a configuration* :



Cliquez ensuite sur le bouton *Next*. Votre nom d'utilisateur (*login*) et votre mot de passe vous sont alors demandés. Ils vous ont été fournis par Scarlet.

Introduisez-les et cliquez sur le bouton *Next*.
Une page confirmant la prise en compte des nouveaux paramètres s'affiche alors :

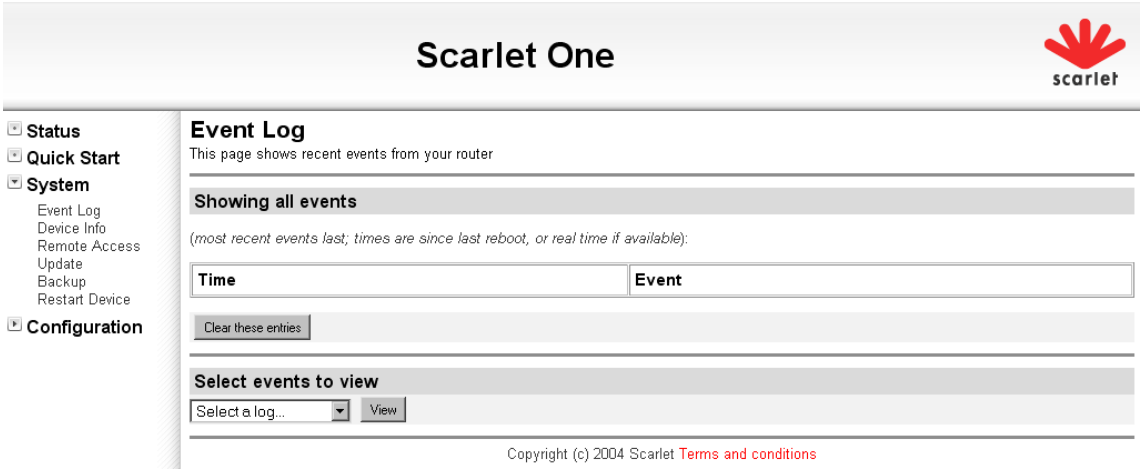

Store Configuration & Restart Device
From this page you may store the configuration and restart your device.
Restart
After restarting, please wait for several seconds to let the system come up. Click on the refresh button of your Web Browser to connect again.
Store

Cliquez sur le bouton *Store*. La configuration sera alors enregistrée et l'appareil redémarrera. Après le redémarrage, la Scarlet Box est configurée pour utiliser le réseau Scarlet et vous pouvez commencer à utiliser votre connexion Internet et la téléphonie Scarlet.

5.3. Options du système – System

Le menu *System* contient des options qui vous fournissent des informations sur la Scarlet Box et vous permettent de gérer et maintenir le système en téléchargeant de nouveaux *firmwares* (logiciel intégré), en téléchargeant des profiles de configuration ou en examinant les *logs* (journaux d'activité).

5.3.1. Journal d'activité - Event Log



Par défaut, cette page affiche une liste des tous les évènements recensés par la Scarlet Box durant la session actuelle. Les types d'évènements suivants sont affichés :

- *Configuration errors* (erreurs de configuration) : ces erreurs sont affichées en rouge dans la liste des évènements.
- *Syslog messages* (erreur de fonctionnement) : ces erreurs sont affichées en noir dans la liste des évènements.

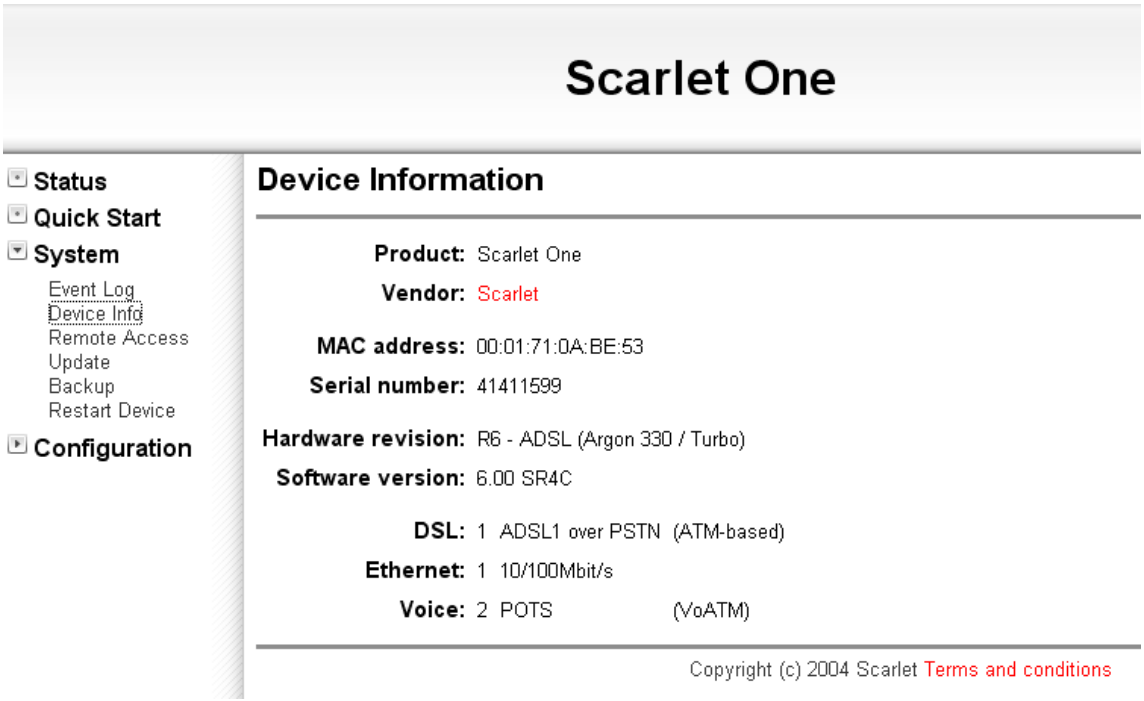
Pour chaque événement recensé dans la liste, les informations suivantes sont fournies :

- Le moment où l'événement a eu lieu (en secondes depuis le redémarrage du système). Note : si vous utilisez le module SNTP, cette colonne affiche l'heure actuelle telle qu'elle est donnée par le serveur SNTP.
- A quel processus l'événement est relié
- Une brève description de l'événement.

Pour vider la liste des évènements, cliquez sur le bouton « *Clear these entries* ».

5.3.2. Informations sur l'appareil - Device Info

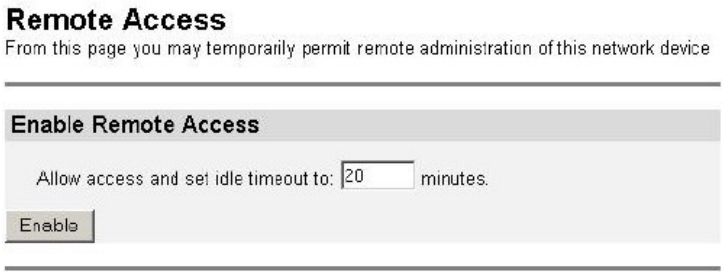
La page *Device Info* propose des informations propres à l'appareil comme le numéro de série, l'adresse MAC (adresse physique Ethernet) et plus encore. Depuis le menu *System*, cliquez sur *Device Info*. La page *Device Info* s'affiche alors.



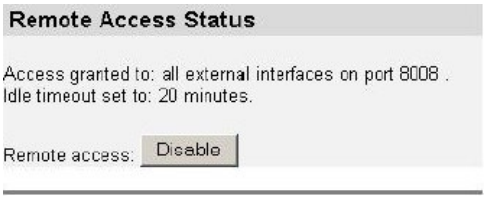
5.3.3. Accès distant - Remote Access

La section *Remote Access* vous permet d'autoriser temporairement un accès distant direct à votre Scarlet Box, ignorant la translation d'adresses (NAT) et le pare-feu (*firewall*). Plus spécifiquement, elle permet à des datagrammes IP d'une station de maintenance adressés à l'interface réseau externe d'outrepasser la translation d'adresses et le pare-feu. Les définitions des stations de maintenance externes peuvent uniquement être manipulées directement via le CLI. Il est nécessaire qu'une station de maintenance enregistre les manipulations effectuées dans la configuration par défaut de la Scarlet Box.
Note : pour configurer un accès distant direct, vous devez d'abord activer le pare-feu (*firewall*).

Une fois que vous avez configuré les paramètres de sécurité, via le menu *Security* du menu *System*, cliquez sur *Remote Access*. La page *Remote Access* s'affiche alors.


Remote Access
From this page you may temporarily permit remote administration of this network device
Enable Remote Access
Allow access and set idle timeout to: 20 minutes.
Enable

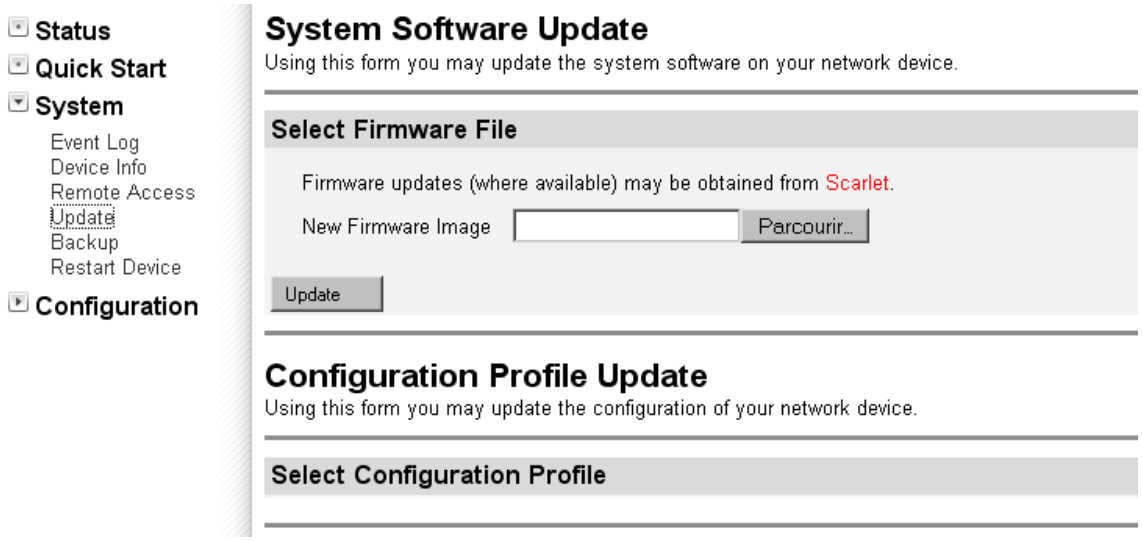
Entrez le temps maximal durant lequel vous souhaitez autoriser l'accès distant. Cliquez alors sur *Enable*. La page *Remote Access Status* s'affiche, confirmant le temps restant pour l'accès distant.


Remote Access Status
Access granted to: all external interfaces on port 8008 .
Idle timeout set to: 20 minutes.
Remote access:
Disable

Vous trouvez ici un bouton *Disable* qui vous permet de mettre fin à un accès distant avant que le temps spécifié soit écoulé. Par exemple, supposons qu'un temps d'expiration de 10 minutes ait été accordé. Ceci permet aux stations de maintenance de se connecter dans les 10 minutes. Si aucune session d'accès distant n'est activée dans le temps imparti, toute tentative d'accès distant ultérieure sera rejetée. Cependant, si une session de maintenance est créée, alors elle aura comme temps limite 10 minutes, qu'il s'agisse d'une session TCP, UDP ou autre. Jusqu'à ce que la session expire, cette station de maintenance ne sera pas déconnectée. Notez qu'une session initiée en TCP peut être terminée avant la fin du temps imparti, car le protocole TCP est un protocole orienté connexion, qui permet la détection de la fin d'une session par le système de sécurité.

5.3.4. Mise à jour du logiciel système

La page *Update* vous permet de charger de nouveaux *firmware* (logiciel système) et d'enregistrer/recharger des profiles de configuration. Dans le menu *System*, cliquez sur *Update*. La page *System Software Update/Configuration Profile Update* s'affiche.



Pour charger un nouveau *firmware*, entrez le nom du fichier contenant le *firmware* dans la boîte *New Firmware Image*, en n'oubliant pas son extension. Si vous ne connaissez pas le nom du fichier avec précision, cliquez sur le bouton *Parcourir* (*Browse* si votre navigateur est en anglais) et choisissez le fichier à l'aide de la fenêtre de sélection de fichier.
Cliquez ensuite sur le bouton *Update*. La page est réaffichée avec les détails du chargement du nouveau *firmware*.

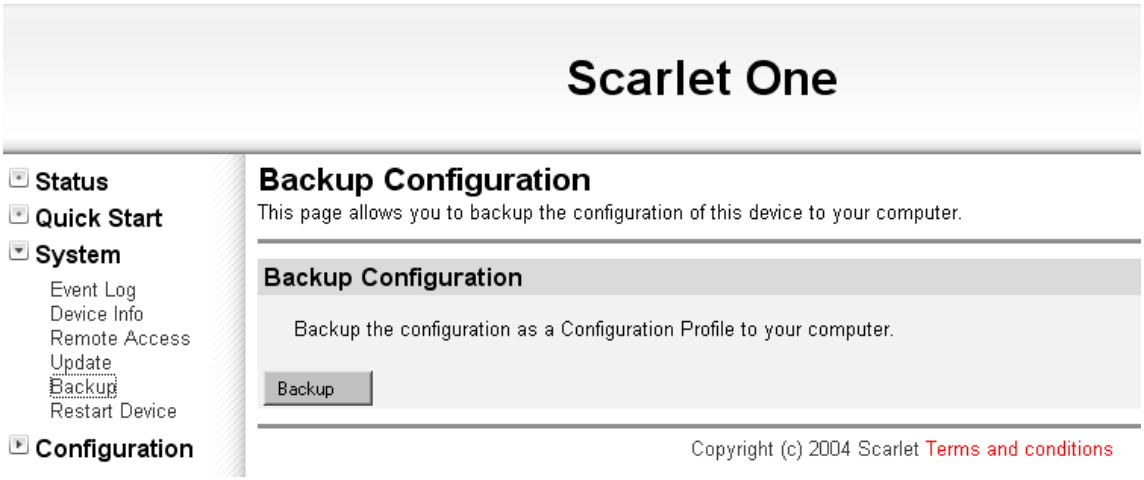
Note : selon le *firmware* actuel et celui que vous chargez, il peut être nécessaire d'entrer un profile de configuration également.

Important : bien que la Scarlet Box soit initialement un produit Allied Data Technologies, utilisez **exclusivement** les *firmwares* délivrés par Scarlet. Vous pouvez les télécharger à l'adresse ftp://ftp.scarlet.be/pub/scarlet/firmware/.

Pour recharger un profile de configuration précédemment sauvé, entrez le nom du fichier dans la boîte *New Configuration Profile*. Si vous ne connaissez pas le nom du fichier avec précision, cliquez sur le bouton *Parcourir* (*Browse* si votre navigateur est en anglais) et choisissez le fichier à l'aide de la fenêtre de sélection de fichier. Cliquez ensuite sur le bouton *Update*. La page est réaffichée avec les détails du chargement du nouveau profile de configuration.

5.3.5. Sauvegarde du profile de configuration

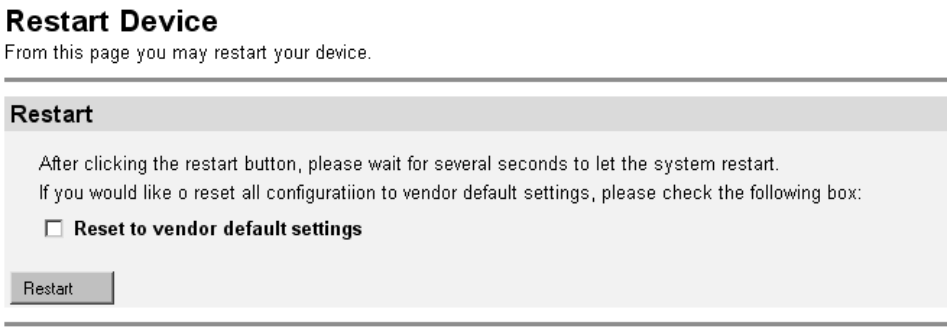
La page *Backup* vous permet de sauvegarder le profile de configuration dans votre ordinateur. A partir du menu *System*, cliquez sur *Backup*. La page *Backup Configuration* s'affiche.



Dans la section *Backup Configuration*, cliquez sur le bouton *Backup*. Une fenêtre de téléchargement de fichier apparaît. Sauvegardez le fichier sur votre disque en suivant la procédure de sauvegarde de fichier de votre navigateur.

5.3.6. Redémarrage de l'appareil – Restart Device

La page *Restart Device* vous permet de redémarrer votre Scarlet Box. A partir du menu *System*, cliquez sur *Restart Device*. La page *Restart Device* s'affiche :


Restart Device
From this page you may restart your device.
Restart
After clicking the restart button, please wait for several seconds to let the system restart.
If you would like o reset all configuratiion to vendor default settings, please check the following box:
Reset to vendor default settings
Restart

Cliquez sur le bouton *Restart* pour provoquer le redémarrage de l'appareil.
Cochez le bouton *Reset to vendor default settings* si vous désirez faire table rase de la configuration. **A n'utiliser qu'en cas de nécessité !**

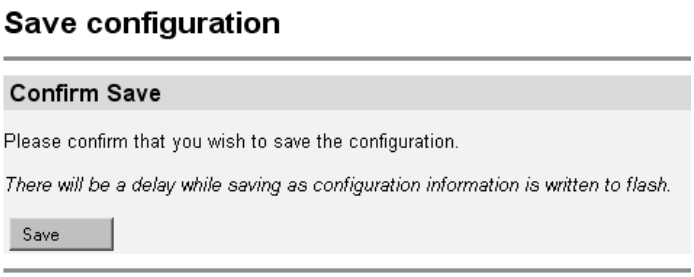
5.4. Configuration

Le menu *Configuration* vous permet d'ajuster les réglages de base et avancés de votre Scarlet Box.

5.4.1. Sauvegarde de la configuration – Save Config

Cette option vous permet d'enregistrer la configuration actuelle dans la mémoire flash de la Scarlet Box. De cette manière, cette configuration sera automatiquement rechargée à chaque démarrage de l'appareil.

A partir du menu *Configuration*, cliquez sur *Save config*. La page suivante s'affiche :


Save configuration
Confirm Save
Please confirm that you wish to save the configuration.
There will be a delay while saving as configuration information is written to flash.
Save

Cliquez sur le bouton *Save* pour enregistrer la configuration dans la mémoire flash, dans le fichier *im.conf* (fichier interne à la Scarlet Box).

Après un moment, la configuration est enregistrée et le message de confirmation suivant s'affiche :

Saved information model to file //flashfs/im.conf

5.4.2. Se connecter au serveur web intégré

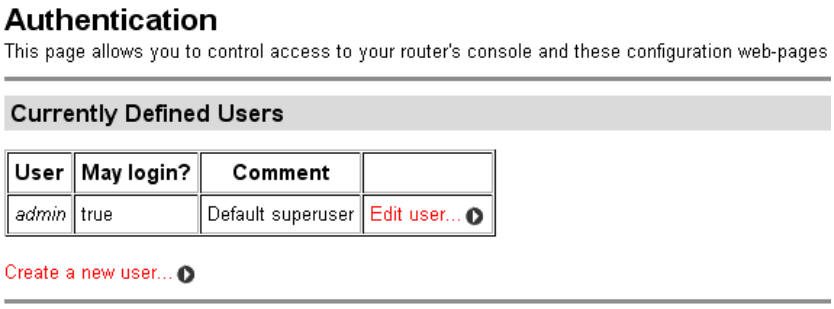
Lorsque vous cliquez la première fois sur une entrée du menu de gauche pour afficher une nouvelle page, une boîte d'identification s'affiche. Vous devez entrer un nom d'utilisateur et un mot de passe pour accéder à ces pages. Les données par défaut sont :

Nom d'utilisateur : **admin**
Mot de passe : **admin**

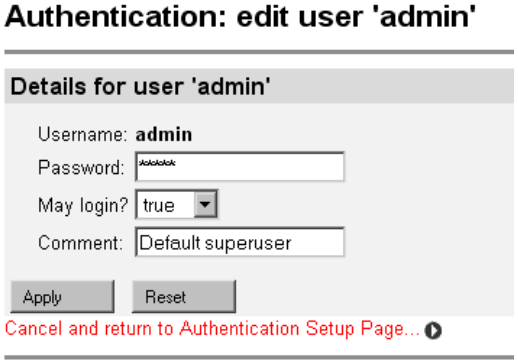
Cliquez ensuite sur *OK*. Vous pouvez alors configurer votre Scarlet Box.

5.4.3. Modifier les paramètres de connexion – Authentication

Pour modifier le nom d'utilisateur et/ou le mot de passe par défaut, ouvrez le menu *Configuration* et cliquez sur *Authentification*. La page *Authentification* s'affiche.



Cette page affiche les utilisateurs actuellement définis. Pour ajouter un nouvel utilisateur, cliquez sur le lien *Create a new user…*. Pour changer le nom d'utilisateur et/ou le mot de passe, cliquez sur le lien *Edit user…* en regard de l'utilisateur que vous désirez modifier. La page *Details for users* s'affiche alors :



Sur cette page, vous pouvez modifier le mot de passe et les droits d'accès de l'utilisateur.

Password : pour entrer un nouveau mot de passe. Assurez-vous que le mot de passe est entré correctement car il s'affiche sous forme masquée.

May login ?: pour autoriser ou refuser l'accès à cet utilisateur. La valeur *True* autorise, la valeur *False* refuse.

Comment : pour entrer un commentaire pour cet utilisateur.

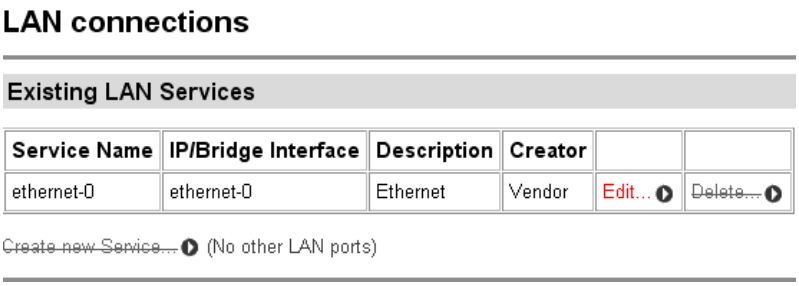
Lorsque les modifications sont terminées, cliquez sur le bouton *Apply* pour les confirmer. Le bouton *Reset* vous permet de faire table rase sur les paramètres.

Pour conserver les nouveaux paramètres définitivement, ouvrez le menu *Configuration* et cliquez sur *Save config* (voir point 5.4.1).

5.5. Connexions réseau – LAN Connection

LAN Connection vous permet de configurer la connexion Ethernet de la Scarlet Box. La connexion Ethernet ne peut être supprimée, seulement éditée.

Ouvrez le menu *Configuration* et cliquez sur *LAN Connection.* La page *LAN Connection* s'affiche :



Cette page montre la liste de toutes les connexions réseau existantes. La liste présente les informations suivantes :

Service name : Nom du port réseau

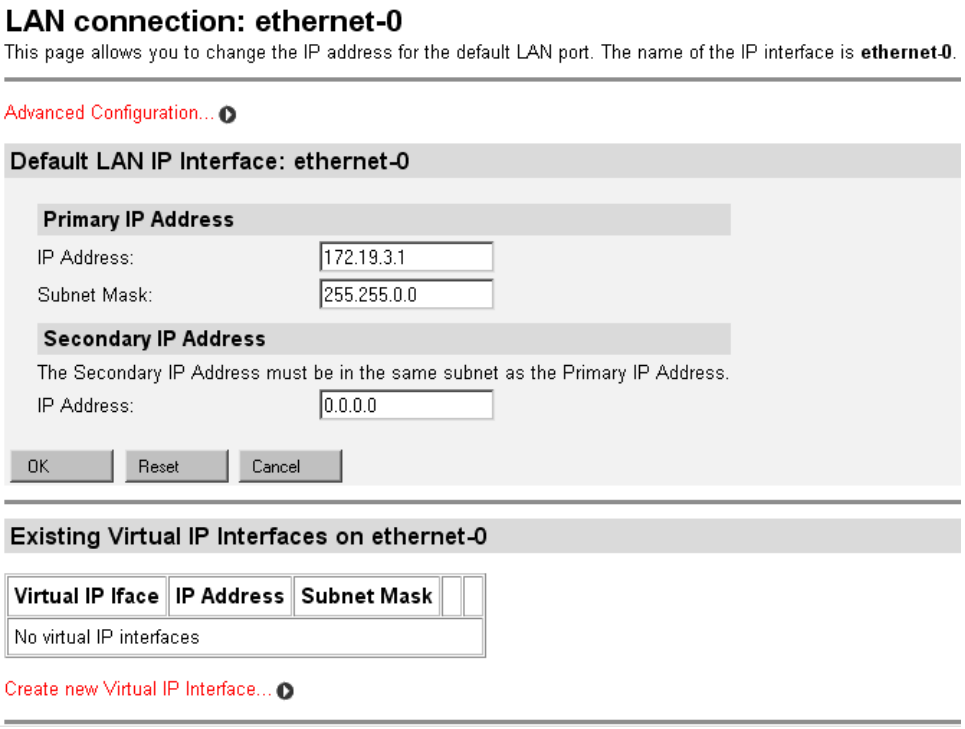
IP/Bridge Interface : Nom interne du port réseau

Description : Description de la connexion.

Creator : A quel niveau d'administration le service a été créé ; CLI, *firmware*, W*ebAdmin* (interface web), ou *factory defaults* (réglages d'usine).

5.5.1. Editer une connexion réseau – Edit a LAN connection

Pour éditer ou mettre à jour votre adresse IP, cliquez sur le lien *Edit* en regard de la connexion réseau que vous souhaitez modifier. La page *LAN Connection* s'affiche :


LAN connection: ethernet-0
This page allows you to change the IP address for the default LAN port. The name of the IP interface is ethernet-0.
Advanced Configuration...
Default LAN IP Interface: ethernet-0
Primary IP Address
IP Address:
172.19.3.1
Subnet Mask:
255.255.0.0
Secondary IP Address
The Secondary IP Address must be in the same subnet as the Primary IP Address.
IP Address:
0.0.0.0
OK
Reset
Cancel
Existing Virtual IP Interfaces on ethernet-0
Virtual IP Iface
IP Address
Subnet Mask
No virtual IP interfaces
Create new Virtual IP Interface...

Cette page contient la table *Default LAN IP interface* :

Primary IP Address :

IP Address : pour configurer l'adresse IP primaire (par défaut)

Subnet Mask : pour configurer le masque de sous-réseau associé à l'adresse IP

Secondary IP Address :

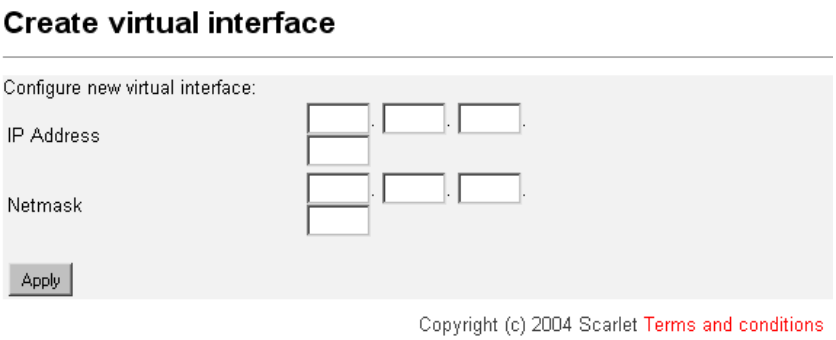
IP Address: pour configurer une adresse IP secondaire. Laissez 0.0.0.0 pour ne définir aucune adresse IP secondaire. Cette deuxième adresse **doit** se trouver dans le même sous-réseau que l'adresse primaire.

Cliquez sur *Reset* si vous désirez effacer les informations présentes, et sur *Cancel* si vous désirez abandonner vos modifications.

Pour obtenir des options avancées pour l'interface, cliquez sur le lien *Advanced Configuration…*

Lorsque vous avez terminé de configurer vos adresses IP, cliquez sur le bouton *OK*. Un message vous confirme la bonne mise à jour des informations relatives aux adresses. Dès ce moment, si vous avez modifié l'adresse IP de votre Scarlet Box, vous pouvez être amené à entrer la nouvelle adresse dans la barre d'adresse de votre navigateur.

Pour ajouter une interface IP virtuelle, cliquez sur le lien *Create new Virtual IP Interface…* . La page *Create virtual interface* s'affiche.



Remplissez les champs destinés à recevoir l'adresse IP et le masque de sous-réseau. L'interface virtuelle peut se placer dans un sous-réseau différent que l'interface Ethernet par défaut. Dès que vous avez terminé d'introduire les informations de la nouvelle interface virtuelle, cliquez sur le bouton *Apply*. Vous reviendrez alors à la page *LAN connections*. La section *Virtual IP Interfaces* offre une liste des interfaces virtuelles. Chaque interface virtuelle est nommée *item#* (ou # est un nombre) par défaut.

Chaque interface virtuelle dispose d'un lien *Edit* (édition) et d'un lien *Delete* (suppression) associés.

Pour éditer une interface virtuelle :

- Cliquez sur le lien *Edit*
- Modifiez les options de l'interface et cliquez ensuite sur le bouton *Apply*.

La page est alors réinitialisée et les nouvelles valeurs sont affichées.
Pour supprimer un service :

- Cliquez sur le lien *Delete*
- Cliquez ensuite sur *Delete this connection*.

Lorsque vous avez terminé la configuration, ouvrez le menu *Configuration* et cliquez sur *Save config* afin d'enregistrer les modifications dans la mémoire de la Scarlet Box (voir point 5.4.1).

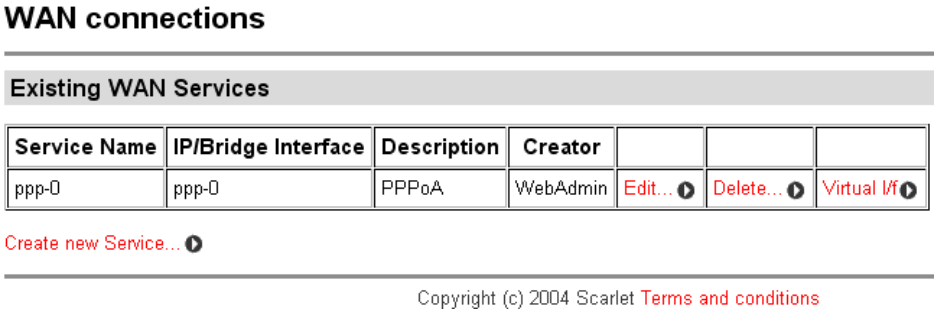
Note : lorsque vous changer l'adresse IP de votre Scarlet Box, assurez-vous que votre carte réseau est bien dans le même sous-réseau que l'adresse de votre Scarlet Box.

5.6. Connexions externes – WAN Connections

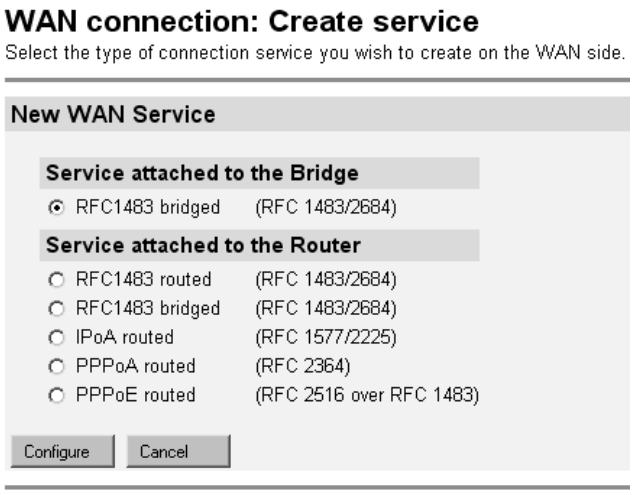
Pour créer une nouvelle connexion DSL, vous devez ajouter une connexion WAN. Selon le réseau de votre fournisseur d'accès, vous devez configurer soit une connexion WAN de pont (*Bridged WAN connection*) ou routée (*Routed WAN Connection*).

Les connexions de pont sont souvent des connexions de type RFC1483 BRIDGED (attachées au pont). Les connexions routées sont souvent des connexions de type RFC1483 ROUTED, PPPoE, PPPoA ou IpoA (attachées au routeur).

Pour créer et configurer des connexions WAN pour votre Scarlet Box, ouvrez le menu *Configuration* et cliquez sur *WAN connections*[1].



Cette page contient une liste des connexions WAN et services qui ont été créés. Pour créer une nouvelle connexion WAN, cliquez sur le lien *Create new Service…*. La page *New WAN Service* s'affiche :


WAN connection: Create service
Select the type of connection service you wish to create on the WAN side.
New WAN Service
Service attached to the Bridge
RFC1483 bridged (RFC 1483/2684)
Service attached to the Router
RFC1483 routed (RFC 1483/2684)
RFC1483 bridged (RFC 1483/2684)
IPoA routed (RFC 1577/2225)
PPPoA routed (RFC 2364)
PPPoE routed (RFC 2516 over RFC 1483)
Configure
Cancel

Cette page affiche une liste des types de connexions WAN disponibles. Choisissez le type de service que vous désirez créer et cliquez sur *Configure*.

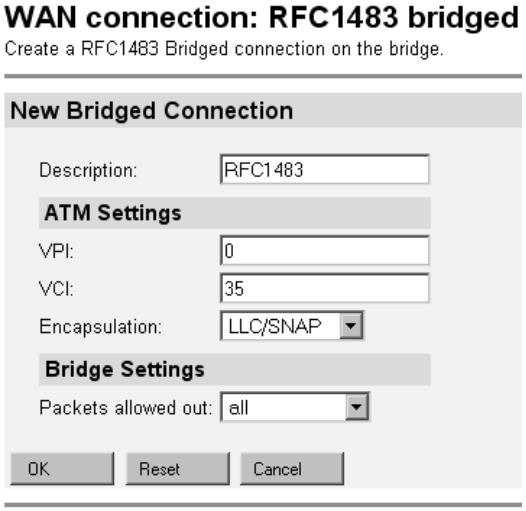
[1] NDT : il est fortement déconseillé de modifier les paramètres par défaut de la configuration Scarlet. Ils conviennent pour la majorité des cas.

5.6.1. Configurer une connexion RFC1483 Bridged

Un des types de connexion les plus utilisés est le type RFC1483 Bridged, attaché au pont. Ce type de connexion fonctionne comme un pont transparent entre la connexion ADSL et la connexion réseau local. Tous les paquets reçus sur une interface sont injectés de manière transparente sur l'autre interface (ADSL vers Ethernet ou vice-versa).

Important : le serveur DHCP doit être **désactivé** pour utiliser la Scarlet Box en mode de connexion de pont RFC1483 Bridged.

Si une connexion RFC1483 Bridged est déclarée, la Scarlet Box route les paquets de et vers les différentes interfaces. Généralement, vous devrez également configurer une translation d'adresse (*NAT*) pour permettre de multiples adresses IP sur l'interface réseau local de la Scarlet Box.



Vous devez fournir des informations détaillées sur le service WAN que vous désirez créer. Votre fournisseur d'accès doit vous délivrer ces informations.

Description : *RFC1483* est le nom par défaut de la connexion WAN.

VPI : *Virtual Path Identifier*, identifiant de chemin virtuel. Il s'agit d'un champ dans l'entête ATM qui permet d'identifier le chemin virtuel auquel un circuit appartient. Le VPI peut prendre toute valeur entre 0 et 4095. Pour Scarlet, la valeur à utiliser est 8.

VCI : *Virtual Channel Identifier*, identifiant de canal virtuel. Il s'agit d'un marqueur qui identifie le canal sur lequel une cellule voyage. Le VCI peut prendre toute valeur entre 1 et 65535. Pour Scarlet, la valeur à utiliser est 35.

Encapsulation : *LLC/SNAP*, soit Ethernet sur LLC/Snap. Il s'agit d'une méthode propre aux connexions de pont, elle est la valeur par défaut pour RFC1483.

Bridge Settings : *Packets allowed out*. Par défaut, tous les paquets sont acceptés : *all*.

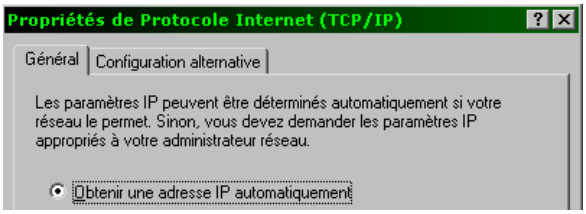
Lorsque vous avez terminé de configurer votre connexion WAN, cliquez sur *OK*. Ouvrez le menu *Configuration* et cliquez sur *Save config*, afin d'enregistrer les nouveaux paramètres dans la mémoire de la Scarlet Box (voir point 5.4.1).

Après avoir configuré votre Scarlet Box en mode RFC1483 Bridged, vous pouvez avoir à configurer les paramètres DHCP de votre carte réseau. DHCP, qui signifie *Dynamic Host Configuration Protocol* (Protocole de configuration dynamique des hôtes), alloue automatiquement une adresse IP à votre carte réseau.

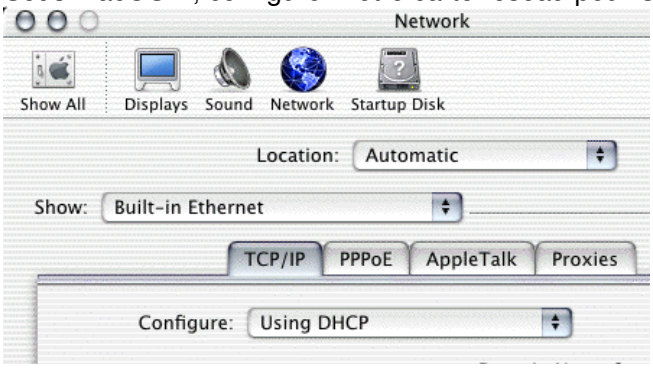
5.6.1.1. Configurer DHCP pour votre carte réseau

Pour configurer votre carte réseau pour utiliser DHCP, référez-vous au manuel de votre système d'exploitation.

Sous Windows, assurez-vous de configurer votre carte réseau pour *Obtenir une adresse IP automatiquement*.


Propriétés de Protocole Internet (TCP/IP)
Général
Configuration alternative
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement

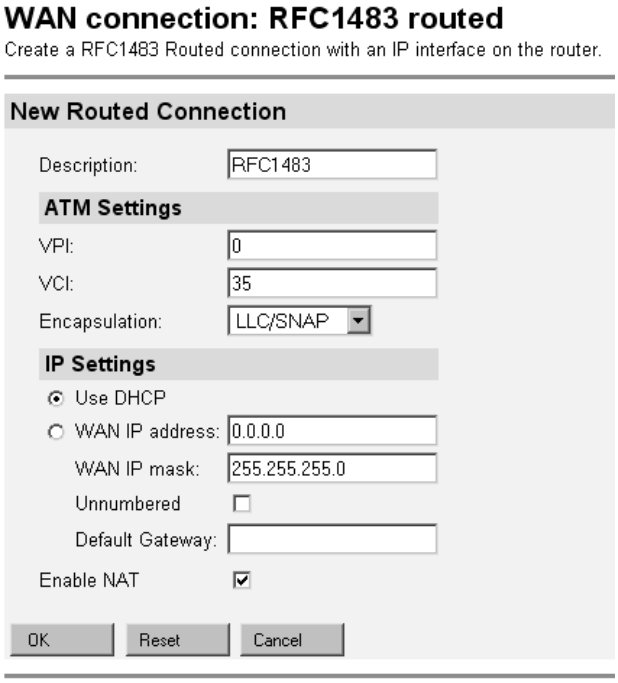
Sous MacOS X, configurez votre carte réseau pour *Utiliser DHCP*.



Sous Linux, consultez le manuel de votre distribution pour déterminer comment configurer votre interface réseau pour utiliser DHCP (ou dhclient).

5.6.2. Configurer une connexion RFC1483 Routed

Une connexion RFC1483 Routed est utilisée lorsque votre fournisseur d'accès offre une connexion routée entre la Scarlet Box et son réseau.



Vous devez fournir des informations détaillées sur le service WAN que vous désirez créer. Votre fournisseur d'accès doit vous délivrer ces informations.

Description : *RFC1483* est le nom par défaut de la connexion WAN.

VPI : *Virtual Path Identifier*, identifiant de chemin virtuel. Il s'agit d'un champ dans l'entête ATM qui permet d'identifier le chemin virtuel auquel un circuit appartient. Le VPI peut prendre toute valeur entre 0 et 4095. Pour Scarlet, la valeur à utiliser est 8.

VCI : *Virtual Channel Identifier*, identifiant de canal virtuel. Il s'agit d'un marqueur qui identifie le canal sur lequel une cellule voyage. Le VCI peut prendre toute valeur entre 1 et 65535. Pour Scarlet, la valeur à utiliser est 35.

Encapsulation : *LLC/SNAP*, soit Ethernet sur LLC/Snap. Il s'agit d'une méthode propre aux connexions de pont, elle est la valeur par défaut pour RFC1483.

Use DHCP : utilisez cette option si votre fournisseur d'accès alloue automatiquement une adresse IP.

WAN IP address : sélectionnez cette option si vous disposez d'une adresse IP WAN fixe. Cette adresse est fournie par votre fournisseur d'accès.

Unnumbered : désactivée par défaut.

Default Gateway : complétez ce champ avec l'adresse de la passerelle par défaut si vous utilisez une adresse IP WAN fixe.

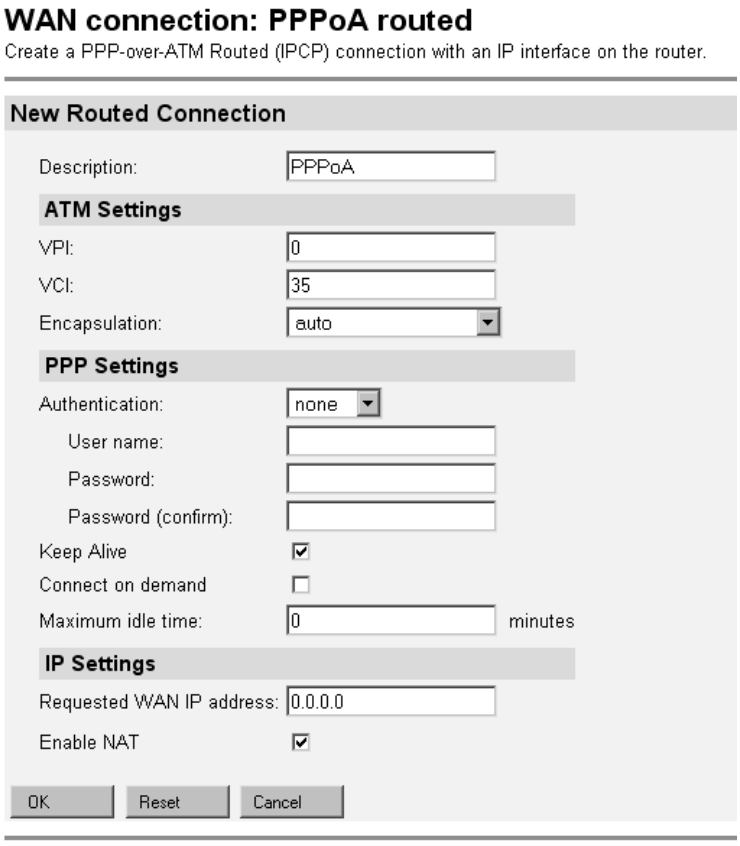
Enable NAT : la translation d'adresses est activée par défaut.

Lorsque vous avez terminé de configurer la connexion WAN, cliquez sur *OK*. Ouvrez le menu *Configuration* et cliquez sur *Save config* afin d'enregistrer les nouveaux paramètres dans la mémoire de votre Scarlet Box (voir point 5.4.1).

5.6.3. Configurer une connexion PPPoA Routed

Les connexions PPPoA Routed sont utilisées principalement quand votre fournisseur d'accès possède un réseau ATM qui requiert une authentification (nom d'utilisateur et mot de passe).

C'est ce type de connexion qu'il faut utiliser avec le réseau Scarlet par défaut.



Description : PPPoA est le nom par défaut de la connexion WAN.

VPI : *Virtual Path Identifier*, identifiant de chemin virtuel. Il s'agit d'un champ dans l'entête ATM qui permet d'identifier le chemin virtuel auquel un circuit appartient. Le VPI peut prendre toute valeur entre 0 et 4095. Pour Scarlet, la valeur à utiliser est 8.

VCI : *Virtual Channel Identifier*, identifiant de canal virtuel. Il s'agit d'un marqueur qui identifie le canal sur lequel une cellule voyage. Le VCI peut prendre toute valeur entre 1 et 65535. Pour Scarlet, la valeur à utiliser est 35.

Encapsulation : *Auto* par défaut.

Authentication : Choisissez la méthode d'authentification utilisée par votre fournisseur d'accès :

None : aucune authentification n'est nécessaire.

PAP : *Password Authentication Protocol*. Le serveur envoie une demande d'authentification à l'utilisateur distant qui se connecte. PAP passe le nom d'utilisateur et le mot de passe non cryptés et identifie le correspondant.

CHAP : *Challenge Handshake Authentication Protocol*. Le serveur envoie une demande d'authentification à l'utilisateur distant qui se connecte. CHAP passe le nom d'utilisateur et le mot de passe cryptés et identifie le correspondant.

Username : entrez le nom d'utilisateur qui vous a été communiqué par votre fournisseur d'accès.

Password : entrez le mot de passe qui vous a été communiqué par votre fournisseur d'accès.

Password (confirm) : entrez à nouveau votre mot de passe, pour confirmation.

Keep alive : activé par défaut.

Connect on demand : désactivé par défaut. Lorsqu'il est activé, le lien PPP est activé automatiquement quand du trafic est envoyé vers le fournisseur d'accès, et désactivé lorsque le trafic a cessé depuis un certain temps. Voir aussi *Maximum Idle Time*.

Maximum idle time : 0 par défaut. Quand l'option *Connect on demand* est activée, cette option représente le temps d'inactivité au bout duquel le lien PPP est déconnecté.

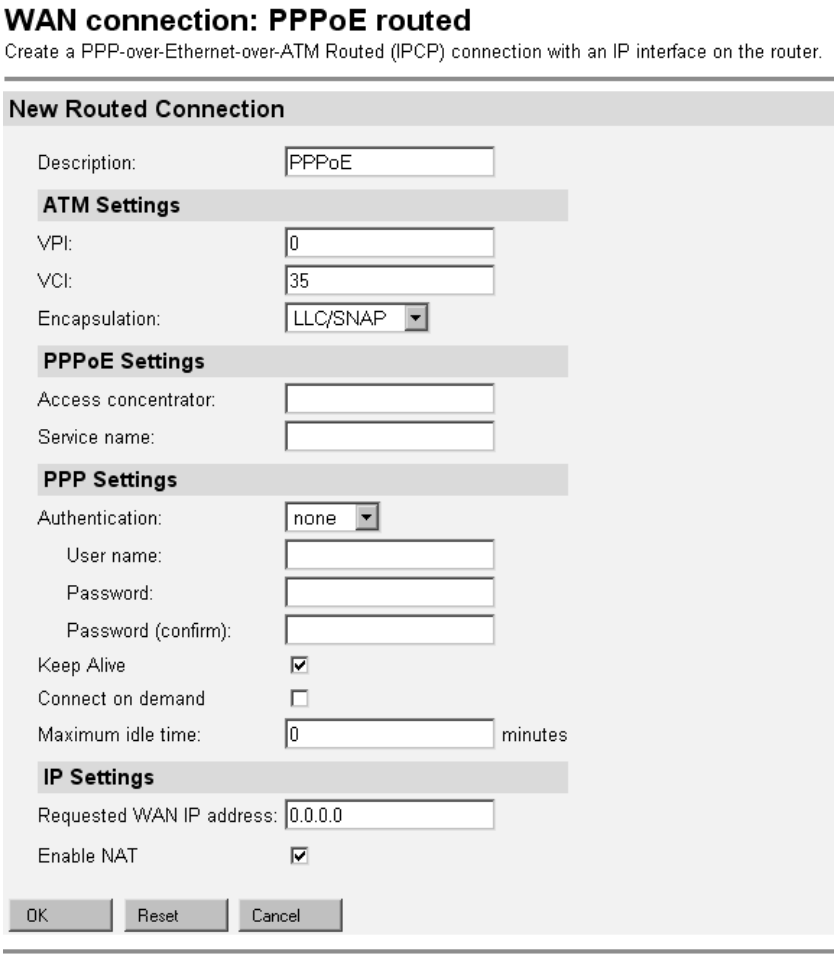
Requested WAN IP address:
Entrez 0.0.0.0 si vous recevez une adresse IP après authentification, ou entrez l'adresse IP fixe fournie par votre fournisseur d'accès.

Enable NAT : la translation d'adresses (*NAT*) est activée par défaut.

Lorsque vous avez terminé de configurer la connexion WAN, cliquez sur *OK*. Ouvrez le menu *Configuration* et cliquez sur *Save config* afin d'enregistrer les nouveaux paramètres dans la mémoire de votre Scarlet Box (voir point 5.4.1).

5.6.4. Configurer une connexion PPPoE Routed

Les connexions PPPoE Routed sont utilisées principalement quand votre fournisseur d'accès possède un réseau Ethernet qui requiert une authentification (nom d'utilisateur et mot de passe).



Description : PPPoE est le nom par défaut de la connexion WAN.

VPI : *Virtual Path Identifier*, identifiant de chemin virtuel. Il s'agit d'un champ dans l'entête ATM qui permet d'identifier le chemin virtuel auquel un circuit appartient. Le VPI peut prendre toute valeur entre 0 et 4095. Pour Scarlet, la valeur à utiliser est 8.

VCI : *Virtual Channel Identifier*, identifiant de canal virtuel. Il s'agit d'un marqueur qui identifie le canal sur lequel une cellule voyage. Le VCI peut prendre toute valeur entre 1 et 65535. Pour Scarlet, la valeur à utiliser est 35.

Encapsulation : *LLC/Snap* par défaut.

Access concentrator :certains fournisseurs d'accès demande cette option. Si votre fournisseur ne vous a pas communiqué ceci, laissez-le blanc.

Service name : certains fournisseurs d'accès demande cette option. Si vous fournisseur ne vous a pas communiqué ceci, laissez-le blanc.

Authentication : Choisissez la méthode d'authentification utilisée par votre fournisseur d'accès :

None : aucune authentification n'est nécessaire.

PAP : *Password Authentication Protocol*. Le serveur envoie une demande d'authentification à l'utilisateur distant qui se connecte. PAP passe le nom d'utilisateur et le mot de passe non cryptés et identifie le correspondant.

CHAP : *Challenge Handshake Authentication Protocol*. Le serveur envoie une demande d'authentification à l'utilisateur distant qui se connecte. CHAP passe le nom d'utilisateur et le mot de passe cryptés et identifie le correspondant.

Username : entrez le nom d'utilisateur qui vous a été communiqué par votre fournisseur d'accès.

Password : entrez le mot de passe qui vous a été communiqué par votre fournisseur d'accès.

Password (confirm) : entrez à nouveau votre mot de passe, pour confirmation.

Keep alive : activé par défaut.

Connect on demand : désactivé par défaut. Lorsqu'il est activé, le lien PPP est activé automatiquement quand du trafic est envoyé vers le fournisseur d'accès, et désactivé lorsque le trafic a cessé depuis un certain temps. Voir aussi *Maximum Idle Time*.

Maximum idle time : 0 par défaut. Quand l'option *Connect on demand* est activée, cette option représente le temps d'inactivité au bout duquel le lien PPP est déconnecté.

Requested WAN IP address:
Entrez 0.0.0.0 si vous recevez une adresse IP après authentification, ou entrez l'adresse IP fixe fournie par votre fournisseur d'accès.

Enable NAT : la translation d'adresses (*NAT*) est activée par défaut.

Lorsque vous avez terminé de configurer la connexion WAN, cliquez sur *OK*. Ouvrez le menu *Configuration* et cliquez sur *Save config* afin d'enregistrer les nouveaux paramètres dans la mémoire de votre Scarlet Box (voir point 5.4.1).

5.7. Sécurité – Security

La Scarlet Box propose des fonctionnalités de sécurité avancées telles qu'un pare-feu à inspection de connexions établies (*Stateful Inspection Firewall*), la translation d'adresses (*NAT*) et des filtres. Une des fonctionnalités les plus utilisées est la translation d'adresses.

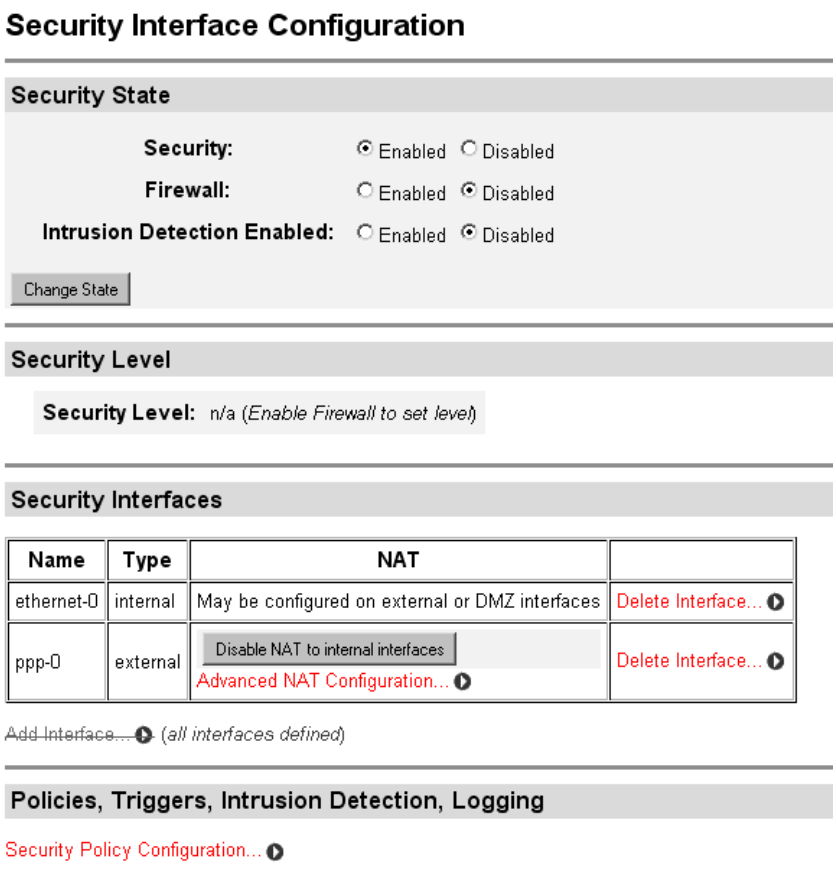
Le menu *Security* vous permet :

- d'activer la sécurité
- d'activer le pare-feu
- d'activer le détecteur d'intrusions
- de configurer les niveaux de sécurité
- de configurer les interfaces de sécurité
- de configurer la politique de sécurité
- de configurer des *Trigger* de sécurité
- de configurer le détecteur d'intrusions
- de configurer l'archivage des informations de sécurité.

Le menu *NAT* vous permet :

- d'activer la translation d'adresses entre des interfaces
- de configurer les adresses globales
- de configurer le mappage inverse (*reverse mapping*).

Ouvrez le menu *Configuration* et choisissez *Security*. La page *Security Interface Configuration* s'affiche :


Security Interface Configuration
Security State
Security: Enabled Disabled
Firewall: Enabled Disabled
Intrusion Detection Enabled: Enabled Disabled
Change State
Security Level
Security Level: n/a (Enable Firewall to set level)
Security Interfaces
Name Type NAT
ethernet-0 internal May be configured on external or DMZ interfaces Delete Interface...
ppp-0 external Disable NAT to internal interfaces Advanced NAT Configuration... Delete Interface...
Add Interface... (all interfaces defined)
Policies, Triggers, Intrusion Detection, Logging
Security Policy Configuration...

Cette page présente les paramètres de sécurité par défaut. Comme toutes les options de sécurité peuvent être configurées, vous devez définir à quelles interfaces vous voulez les appliquer. Les interfaces déjà configurées l'ont été par Scarlet. Il est fortement recommandé de laisser ces paramètres **par défaut**, à moins que vous ne sachiez exactement ce que vous faites.

5.7.1. Activation de la sécurité

Vous devez activer *Security* avant de pouvoir ajouter des fonctionnalités de sécurité comme le pare-feu, la translation d'adresses ou les filtres.

Dans la section *Security State* :
Cliquez sur le bouton radio *Security Enabled* et sur le bouton *Change State* pour mettre à jour la section *State*. La sécurité générale est maintenant activée.

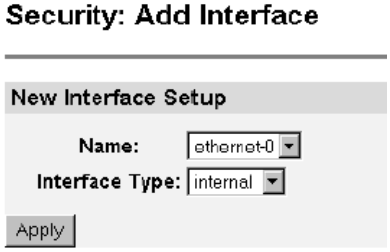
5.7.2. Configuration des interfaces sécurisées

Avant que les options de sécurité ne puissent être configurées, il doit exister au moins 2 interfaces définies et configurées. Les interfaces sécurisées représentent les connexions logiques de et vers la Scarlet Box. Les interfaces sécurisées sont utilisées pour activer la sécurité sur ces connexions.

Il existe 3 types d'interfaces sécurisées différents :
- Internes (*internal*) : habituellement la connexion réseau
- Externes (*external*) : habituellement la connexion WAN (ADSL)
- DMZ : habituellement une deuxième connexion réseau ou un sous-réseau IP

Important : lorsqu'une connexion WAN est déjà configurée avec la translation d'adresses active, les interfaces sécurisées interne et externe sont automatiquement ajoutées et configurées. Ces interfaces sécurisées peuvent être utilisées pour activer les autres options de sécurité.

Pour ajouter une interface sécurisée, ouvrez le menu *Configuration* et cliquez sur *Security*. La page *Security Interface Configuration* s'affiche. Choisissez *Add Interface* dans la section *Security Interfaces.* La page *Security : Add interface* s'affiche :



Sélectionnez la connexion WAN ou LAN appropriée depuis la liste *Name*.
- La connexion réseau Ethernet est désignée par *ethernet-0.*
- Les connexions WAN sont désignées comme *ppp-0*, *rfc1483-0* ou *ipoa-0.*

Sélectionnez ensuite le type d'interface (*Interface type*) adéquat. Généralement, les connexions réseau *ethernet-0* ou *ethernet-1* sont de type *internal*. Les connexions WAN sont généralement de type *external*.

Cliquez sur le bouton *Apply* pour ajouter l'interface sécurisée.

La page *Security Interface Configuration* s'affiche, dans laquelle la nouvelle interface sécurisée a été ajoutée à la liste *Security Interfaces* :

Security Interfaces

Name	Type	NAT	
ethernet-0	internal	May be configured on external or DMZ interfaces	Delete Interface...

5.7.3. Configuration de la translation d'adresses (NAT)

La technique de translation d'adresses (*NAT, Network Address Translator*) implémente la translation des adresses par ports (*PAT, Port Address Translation*) et fournit une translation des adresses réseau par ports (*NATP, Network Address Port Translation*), également connue comme masquage d'IP (*IP Masquerading*). Elle permet à une seule adresse IP réelle sur un WAN (réseau ADSL) d'être partagée par plusieurs appareils côté réseau interne, chacun disposant d'une adresse privée.

La translation d'adresses peut être activée directement en configurant une connexion WAN. Voyez la section 5.6 pour plus de détails).

Si la translation d'adresse n'a pas été activée durant la configuration d'une connexion WAN, ouvrez le menu *Configuration* et cliquez sur *WAN Connections.* La page *WAN Connections* s'affiche. Editez la connexion WAN en cliquant sur le lien *Edit…*. La page *WAN Connection : edit* s'affiche :

Edit connection: 'ppp-0'

Service	PPP	ATM Channel	IP Interface

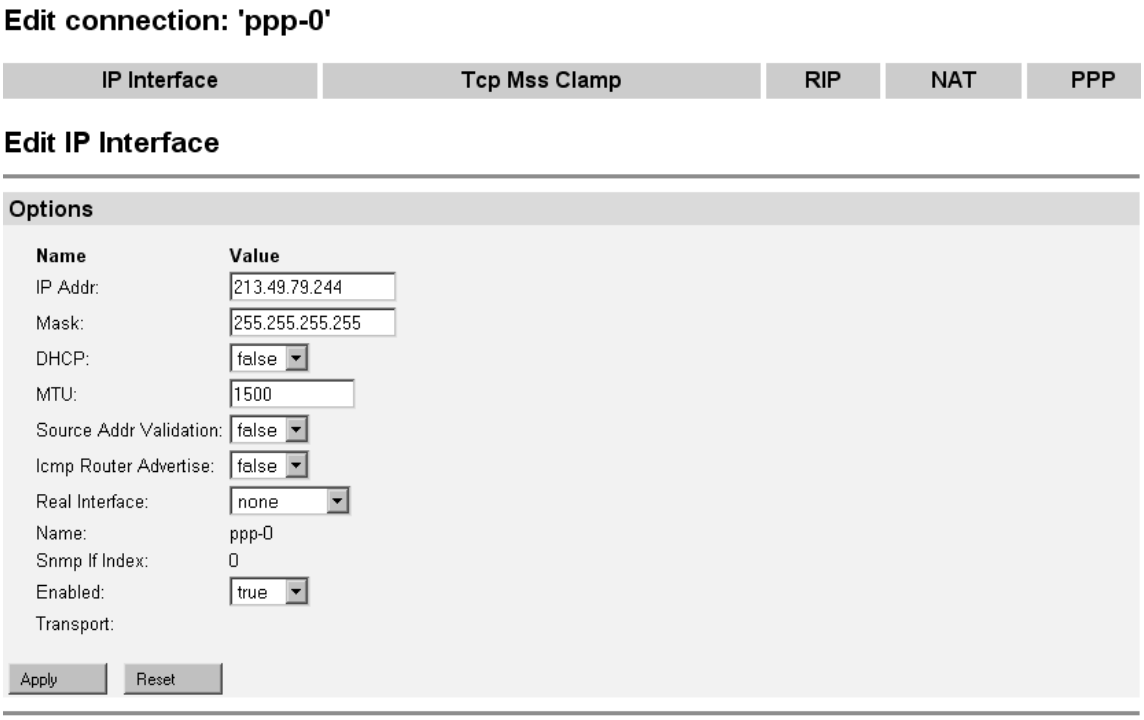
Edit Service

Options

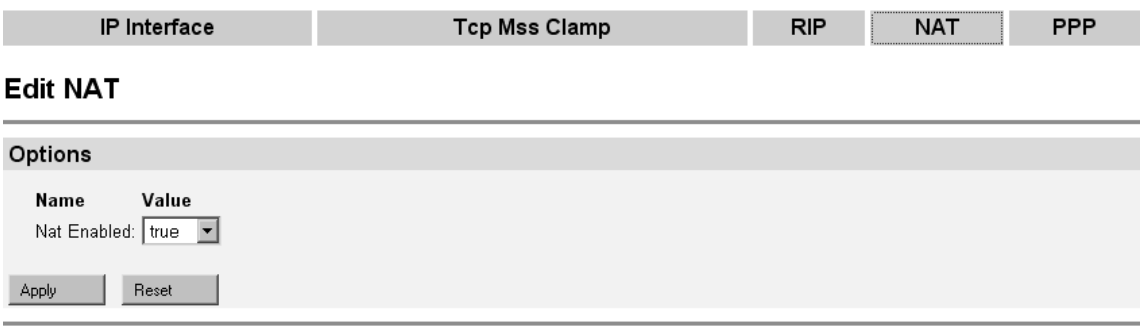
Name	Value
Creator:	WebAdmin
Description:	PPPoA
ATM Protocol:	PPPoA
Ether Protocol:	None

Apply Reset

Cliquez sur l'onglet *IP Interface*. La page *Edit IP Interface s'affiche.*



Cliquez sur l'onglet *NAT* . La page *Edit NAT* s'affiche :



Sur cette page, la translation d'adresses peut être activée ou désactivée. Cliquez sur la liste *NAT Enabled* :

- *True* : la translation d'adresses est activée
- *False* : la translation d'adresses est désactivée.

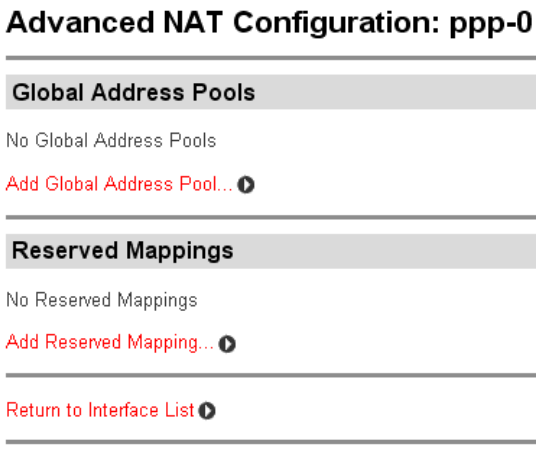
Après que vous ayez modifié un paramètre, cliquez sur le bouton *Apply*. N'oubliez pas d'enregistrer vos modifications. Ouvrez le menu *Configuration* et cliquez sur *Save config* pour enregistrer vos nouveaux paramètres dans la mémoire de la Scarlet Box (voir point 5.4.1).

5.7.3.1. Réserver des affectations dans la translation d'adresses

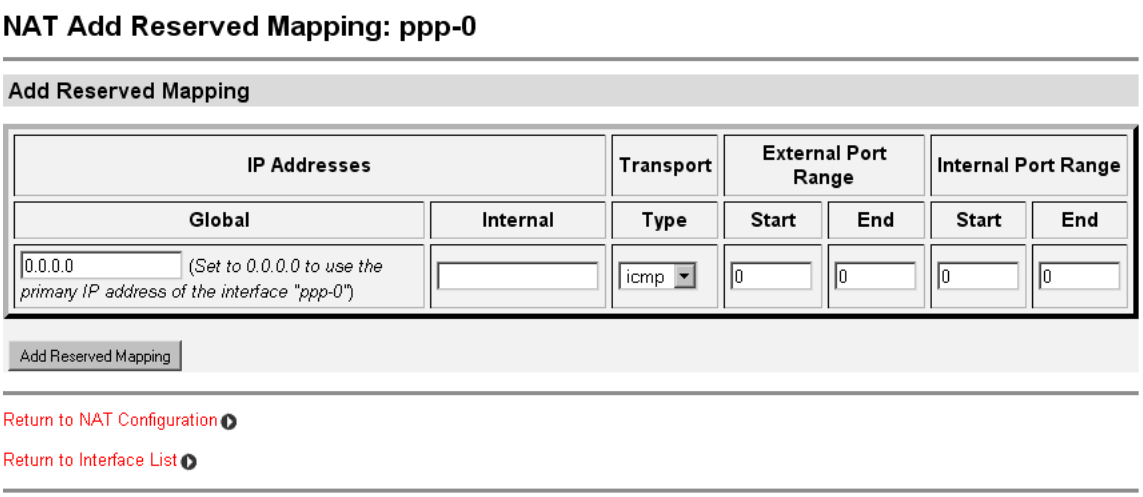
La réservation d'affectations (*NAT reserved* mapping) vous permet d'affecter une interface sécurisée externe ou une adresse IP d'un ensemble global à une adresse IP individuelle à

l'intérieur du réseau. L'affectation est basée sur le type de transport et le numéro de port. Avant de pouvoir réserver une affectation, vous devez configurer la translation d'adresses. Voyez la section 5.7.3.

Pour effectuer une réservation d'affectation sur les interfaces qui utilisent déjà la translation d'adresses, ouvrez le menu *Configuration* et cliquez sur *Security*. Dans la liste *Security Interfaces*, cliquez sur le lien *Advanced NAT Configuration* en regard de l'interface à laquelle vous souhaitez ajouter une réservation d'affectation. La page *Advanced NAT Configuration* s'affiche :



Cliquez sur le lien *Add Reserved Mapping*. La page *Add Reserved Mapping* s'affiche:



Cette page vous permet de configurer vos réservation d'affectation. Entrez les valeurs nécessaires dans les champs suivants :

Global IP Address : si vous affectez depuis une adresse IP globale, entrez-la ici. Si vous affectez à partir d'une interface sécurisée, entrez 0.0.0.0.

Internal IP Address : entrez ici l'adresse IP de l'hôte individuel à l'intérieur de votre réseau.

Transport Type : choisissez ici le type de transport que vous désirez affecter de l'interface externe à l'interface interne.

External Port Range / Internal Port Range : l'intervalle de ports que votre transport utilise. Si vous désirez affecter un seul port, entrez uniquement le port externe de début (*External Start Port*).

Lorsque vous avez terminé de configurer vos réservations, cliquez sur *Add reserved mapping*. La page est rechargée et les nouvelles réservations sont ajoutées à votre configuration NAT.

Important : assurez-vous que l'adresse IP interne est dans le même sous-réseau sur l'adresse IP de votre Scarlet Box.

Pour supprimer une réservation d'affectation, cliquez sur le lien *Delete*. La page *Delete Reserved Mapping Confirmation* s'affiche. Cliquez sur le bouton *Delete Reserved Mapping*. La réservation est alors supprimée.

N'oubliez pas d'enregistrer vos modifications. Ouvrez le menu *Configuration* et cliquez sur *Save Config* afin d'enregistrer vos nouveaux paramètres dans la mémoire de la Scarlet Box (voir point 5.4.1).

5.7.4. Activation du pare-feu (*firewall*)

Avant d'activer la pare-feu, vous devez avoir activé la sécurité (*Security enabled*) et vous devez avoir au moins **1 interface interne** ou **1 interface externe** configurée. Assurez-vous que les connexions WAN et réseau (*LAN*) et que les interfaces sécurisées sont définies et configurées.

Pour activer le pare-feu, rendez-vous sur la section *Security State* et sélectionnez *Firewall enabled*. Cliquez sur *Change State* pour confirmer et mettre à jour la section *Security State*. Le pare-feu est maintenant activé sur la Scarlet Box.

IMPORTANT : activer le pare-feu bloque **TOUT TRAFFIC** entrant ou sortant de la Scarlet Box. Des règles de pare-feu doivent être configurées pour permettre le passage du traffic.

5.7.5. Activer la détection d'intrusions

Avant d'activer la détection d'intrusions, vous devez avoir activé la sécurité (*Security enabled*) et vous devez avoir au moins **1 interface interne** ou **1 interface externe** configurée. Assurez-vous que les connexions WAN et réseau (*LAN*) et que les interfaces sécurisées sont définies et configurées.

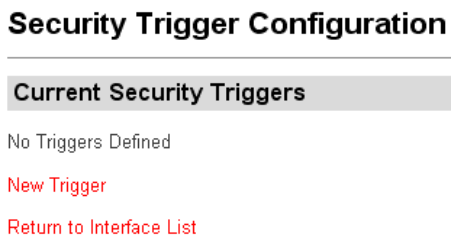
Pour activer la détection d'intrusions, rendez-vous sur la section *Security State* et sélectionnez *Intrusion Detection enabled*. Cliquez sur *Change State* pour confirmer et mettre à jour la section *Security State*.
La détection d'intrusion est maintenant activée sur la Scarlet Box.

5.7.6. Configuration des *triggers*

Un *trigger* permet à une application d'ouvrir un port secondaire pour transporter des paquets. Les applications les plus courantes nécessitant des ports secondaires sont *FTP* et *NetMeeting***.** Les *triggers* sont obligatoires pour permettre à ces applications de fonctionner correctement avec une translation d'adresses ou d'autres options de sécurité.

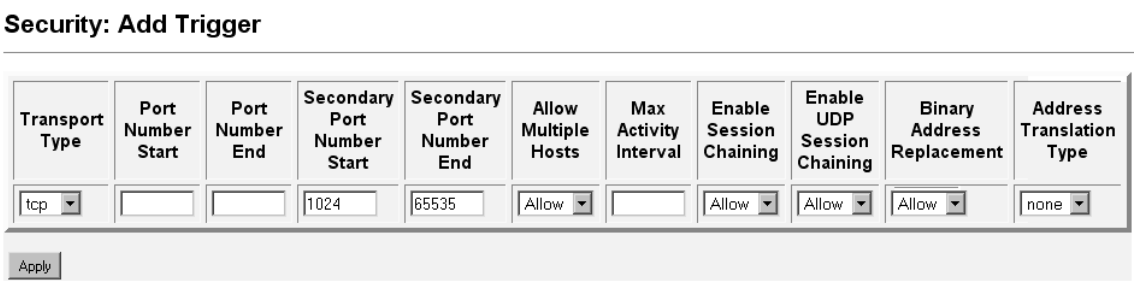
Cette section suppose que vous avez activé la sécurité et défini au moins une interface sécurisée.

Pour configurer un *trigger*, dans la section *Policies, Triggers and Intrusion Detection* sous *Security Interface Configuration*, cliquez sur *Security Trigger Configuration*. La page *Security Trigger Configuration* s'affiche :



5.7.6.1. Ajouter un *trigger*

Pour ajouter un *trigger*, cliquez sur le lien *New trigger*. La page *Security Add Trigger* s'affiche:



Une liste d'options s'affiche, permettant de configurer le *trigger* :

Transport type : sélectionnez un type de transport selon que vous ajoutez un *trigger* pour une application TCP ou UDP.

Port Number Start : entrez la borne inférieure de l'intervalle de ports que la session primaire utilise.

Port Number End : entrez la borne supérieure de l'intervalle de ports que la session primaire utilise.

Secondary Port Number Start
entrez la borne inférieure de l'intervalle de ports que la session secondaire utilise.

Secondary Port Number End
entrez la borne supérieure de l'intervalle de ports que la session secondaire utilise.

Allow Multiple Hosts : sélectionnez *Allow* si vous désirez permettre à la session secondaire d'être initiée de/vers différents hôtes. Sélectionnez *Block* si vous

désirez que la session secondaire soit initiée uniquement de/vers un même hôte distant. Par défaut : *Allow*.

Max Activity Interval : entrez l'intervalle de temps maximum (en millisecondes) entre l'utilisation de sessions secondaires. Par défaut : 10000.

Enable Session Chaining :
Sélectionnez *Allow* ou *Block* selon que vous acceptez ou pas le chaînage de sessions TCP sur plusieurs niveaux. Par défaut : *Allow*.

Enable UDP Session Chaining :
Sélectionnez *Allow* ou *Block* selon que vous acceptez ou pas le chaînage de sessions UDP et TCP sur plusieurs niveaux. Vous devez avoir placé *Enable Session Chaining* sur *Allow* pour utiliser cette option. Par défaut : *Allow*.

Binary Address Replacement :
Sélectionnez *Allow* ou *Block* selon que vous désirez ou pas utiliser le remplacement d'adresses binaires sur un *trigger* existant. Par défaut : *Allow*.

Address Translation Type :
Spécifiez quel type de remplacement d'adresses est apposé sur un *trigger*. Vous devez avoir placé *Binary Adress Replacement* sur *Allow* pour utiliser cette option. Par défaut : *None*.

Lorsque vous avez terminé de configurer un *trigger*, cliquez sur *Apply*. La page *Firewall Trigger Configuration* s'affiche, contenant les détails du *trigger* que vous venez de configurer.

5.7.6.2. Supprimer un *trigger*

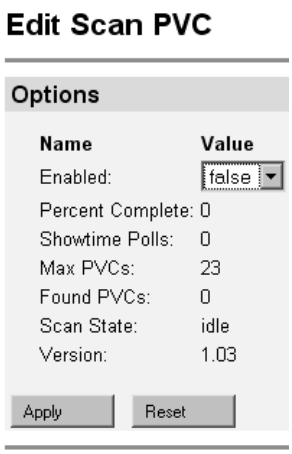
Chaque *trigger* affiché dans la page *Firewall Trigger Configuration* possède un lien *Delete* qui lui est assigné. Pour supprimer un *trigger*, cliquez sur ce lien. La page *Confirmation* s'affiche. Cliquez sur le bouton *Delete* pour supprimer le *trigger*.

La page *Firewall Trigger Configuration* s'affiche alors. Les détails du *trigger* que vous venez de supprimer ont disparu.

5.8. Chercher un service – Search Service

Le menu *Search Service* vous permet d'enclencher un dispositif de détection d'une liste fixe de PVCs à la recherche de protocoles comme RFC1483, PPPoA et PPPoE. Il crée automatiquement les transports idoines et les attache à la pile IP.

A partir du menu *Configuration*, cliquez sur *Search service*. La page *Edit Scan PVC* s'affiche :



Cliquez sur la liste déroulante *Value* et sélectionnez *True*. Cliquez ensuite sur le bouton *Apply*. La détection démarre et les différents paramètres sur la page suivent le statut de la détection :

- *Percent Complete* : affiche la progression de la détection (en pourcentage)
- *Showtime polls* : nombre de fois que la synchronisation DSL est vérifiée
- *Max PVCs* : nombre maximal de PVCs que la détection doit examiner
- *Found PVCs* : nombre de PVCs découverts par la détection
- *Scan State* :
  idle (pas en train de détecter)
  watingForResponse (en train de détecter)
  waitingForShowtime (en train d'examiner une synchronisation DSL)
  Aborted (la détection a été interrompue avant terme)
  FoundPVC (la détection est terminée – au moins un PVC découvert)
  npPVCsFound (la détection est terminée – aucun PVC découvert)
- *Version* : version du module de détection

5.9. Pont PPP sans installation – Zero Installation PPP Bridge (ZIPB)

Dynamic ZIPB, aussi nommé *PPP Half Bridge*, permet à un utilisateur de partager l'adresse IP publique assignée par son fournisseur d'accès avec un ordinateur sur son réseau. Ceci évite les problèmes engendrés par certaines applications lorsqu'elles fonctionnent derrière une translation d'adresses, et évite d'avoir à exécuter une pile PPP sur l'ordinateur. Ce n'est pas vraiment un pont, mais plutôt un routage d'IP avec des capacités de gestion d'adresses spéciales.

5.9.1. ZIPB dans les configuration utilisant un pont

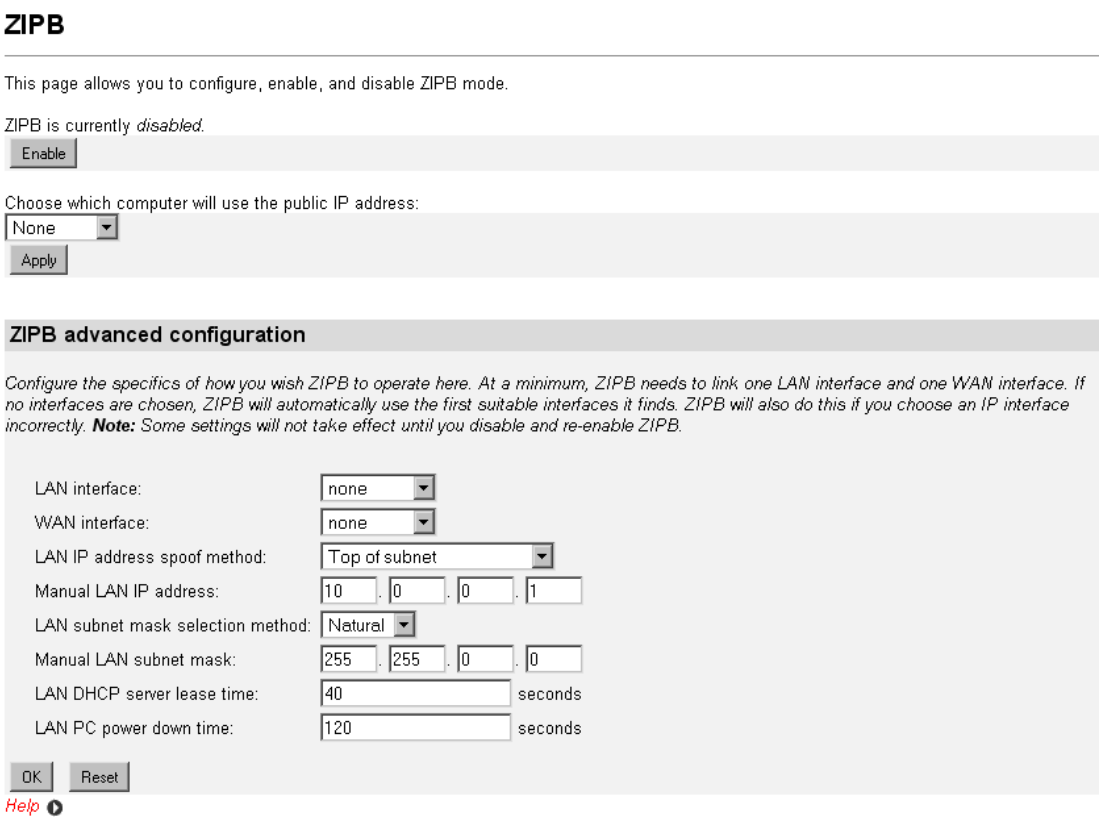
Dans certaines configurations utilisant un pont, un client *PPPoE*/*PPPoA* doit être installé sur chaque ordinateur appartenant au réseau local. Aucune adresse IP publique n'est assignée à la Scarlet Box, chaque ordinateur utilise une adresse IP publique directement.
L 'activation de *ZIPB* dans une configuration utilisant un pont dispense d'installer un client *PPPoE* sur chaque ordinateur du réseau local, car la Scarlet Box dispose déjà d'un client *PPPoE/PPPoA* embarqué.

5.9.2. ZIPB dans les configuration utilisant une translation d'adresses

En mode translation d'adresses/routage, le client *PPPoE/PPPoA* réside dans la Scarlet Box. La Scarlet Box utilise l'adresse IP fournie par le fournisseur d'accès et la translation d'adresses définit un sous-réseau sur le réseau local. Lorsque la translation d'adresses est utilisée, des troubles peuvent apparaître dans certaines applications typiques qui ne sont pas prévues pour fonctionner comme cela. Lorsqu'on permet à un ordinateur sur le réseau de s'accaparer l'adresse IP publique fournie par le fournisseur d'accès, ces applications peuvent fonctionner sans avoir à subir une translation d'adresses. Les autres ordinateurs sur le réseau accèdent normalement au réseau externe (ADSL) à travers la translation d'adresses.

5.9.3. Activer/désactiver ZIPB

Pour activer ou désactiver ZIPB, ouvrez le menu *Configuration* et cliquez sur *ZIPB*. La page *ZIPB* s'affiche :


ZIPB
This page allows you to configure, enable, and disable ZIPB mode.
ZIPB is currently disabled.
Enable
Choose which computer will use the public IP address:
None
Apply
ZIPB advanced configuration
Configure the specifics of how you wish ZIPB to operate here. At a minimum, ZIPB needs to link one LAN interface and one WAN interface. If no interfaces are chosen, ZIPB will automatically use the first suitable interfaces it finds. ZIPB will also do this if you choose an IP interface incorrectly. Note: Some settings will not take effect until you disable and re-enable ZIPB.
LAN interface:
none
WAN interface:
none
LAN IP address spoof method:
Top of subnet
Manual LAN IP address:
10 . 0 . 0 . 1
LAN subnet mask selection method:
Natural
Manual LAN subnet mask:
255 . 255 . 0 . 0
LAN DHCP server lease time:
40
seconds
LAN PC power down time:
120
seconds
OK
Reset
Help

Cliquez sur le bouton *Enable* pour activer ZIPB. Cliquez ensuite sur la liste déroulante *Choose which computer will use the public IP adress* et sélectionnez un ordinateur du réseau. L'adresse IP publique WAN sera alors partagée avec cet ordinateur, et ce dernier n'aura plus besoin de passer par la translation d'adresses. Cliquez enfin sur *Apply*.

Dès que la Scarlet Box a déterminé l'adresse IP publique à l'aide de *IPCP*, *ZIPB* crée une adresse IP virtuelle et l'assigne à une interface virtuelle attachée à l'interface Ethernet de la Scarlet Box. Le serveur *DHCP* est alors mis à jour pour permettre à l'ordinateur sélectionné d'obtenir l'adresse IP publique et les adresses des serveurs DNS publics lors du prochain renouvellement de bail par *DHCP*.

Cliquez sur le bouton *Disable* pour désactiver *ZIPB* à nouveau.

5.9.4. Configuration avancée de ZIPB – ZIPB Advanced configuration

Note : assurez-vous que *ZIPB* est désactivé avant de procéder à toute modification de configuration. Dès que vous avez terminé vos modifications et cliqué sur *OK*, vous pouvez activer *ZIPB*. Les changements effectués seront alors reportés dans la configuration. Toute modification à la configuration effectuée alors que *ZIPB* est actif ne sera pas prise en compte.

Vous pouvez configurer les paramètres avancés suivants :

LAN interface : sélectionnez l'interface LAN réseau local sur laquelle *ZIPB* fonctionnera. Généralement *ethernet-0.*

WAN interface : sélectionnez l'interface WAN sur laquelle *ZIPB* fonctionnera. Généralement *ppp-0*.

LAN IP address spoof method:
Configure la méthode avec laquelle les adresses IP virtuelles sont créées sur le réseau local. Lorsqu'une adresse IP publique est assignée à un ordinateur sur le réseau local, une adresse IP appartenant au même sous-réseau que l'adresse IP publique doit être créée et assignée à l'interface LAN de la Scarlet Box (ceci afin de servir de passerelle). Cette option permet de choisir comment cette adresse IP est créée. Cliquez sur la liste déroulante *LAN IP address spoof method* et sélectionnez une des options :

Top of subnet : choisir l'adresse IP la plus élevée dans le sous-réseau
Bottom of subnet : choisir l'adresse IP la plus basse dans le sous-réseau
Increment : incrémenter l'adresse IP assignée de 1
Manual : choisir l'adresse IP spécifiée dans le champ *Manuel LAN IP address*.
Uses PPP server address: utiliser l'adresse IP du serveur PPP.

Manual LAN IP address :
Détermine l'adresse IP manuelle à utiliser, uniquement si vous avez choisi la méthode *Manual* dans la liste *LAN IP address spoof method*.

LAN subnet mask selection method:
Définit la méthode avec laquelle le masque de sous-réseau est déterminé. Vous pouvez choisir parmi ces deux méthodes :
Natural : utilise le masque de sous-réseau propre à l'adresse IP assignée.
Manual : utilise le masque de sous-réseau défini dans le champ *Manual LAN subnet mask*.

Manual LAN subnet mask :
Détermine un masque de sous-réseau manuel, uniquement si vous avez choisi *Manual* dans la liste *LAN subnet mask selection method*.

LAN DHCP server lease time :
Détermine le temps accordé à un bail *DHCP* sur le réseau local à partir du serveur *DHCP*, en secondes.

LAN PC power down time:
Détermine le temps d'inactivité au bout duquel un ordinateur du réseau local ayant reçu l'adresse IP publique est considéré comme éteint et n'a donc plus besoin de l'accès à Internet.

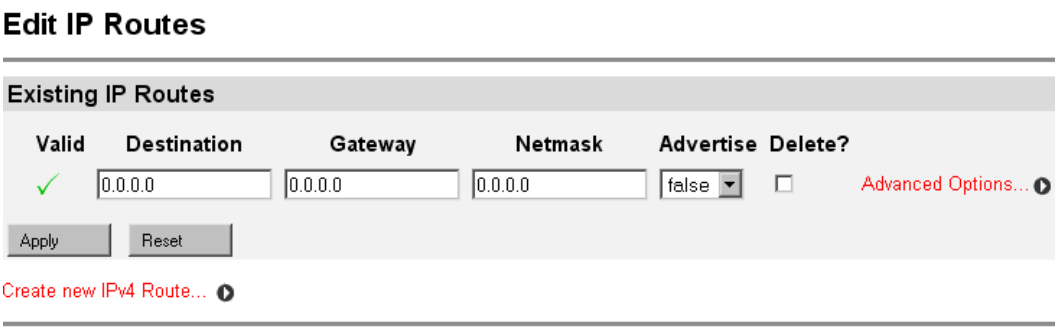
Une fois que vous avez configuré *ZIPB*, cliquez sur le bouton *OK*. Notez bien que les modifications de configuration ne prendront effet que lorsque *ZIPB* est réactivé. Cliquez sur le bouton *Enable* en haut de la page.

5.9.5. Limitations de ZIPB

Lorsque *ZIPB* est actif, tout trafic émanant de votre Scarlet Box, comme les *pings* ou les demandes de confirmation d'activité en provenance d'Internet, ne recevront pas de réponse. Cela est dû au fait que ce trafic semblera venir de l'adresse IP publique et sera dès lors rerouté vers l'ordinateur qui partage l'adresse IP publique. Il n'y a que le trafic émanant de l'ordinateur sur le réseau qui peut être routé en retour.

5.10. Routes IP – IP Routes

Cette option vous permet de créer des routes statiques vers des adresses IP à travers le nom d'une interface ou l'adresse d'une passerelle. Ouvrez le menu *Configuration* et cliquez sur *IP Routes*. La page *Edit Routes* s'affiche :



Cette page affiche les informations suivantes à propos des routes existantes :

- Si la route est valide ✓ ou invalide ✗
- L'adresse IP de destination
- L'adresse de la passerelle (*Gateway*)
- Le masque de sous-réseau (*Netmask*)

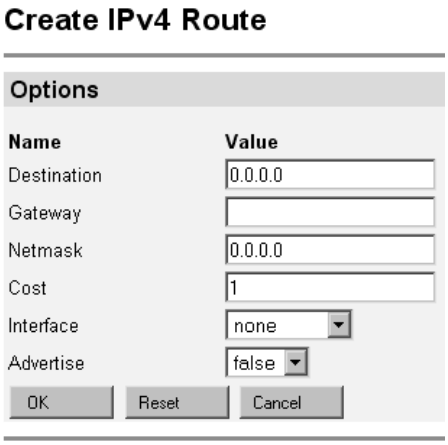
Pour éditer une destination, une passerelle ou un masque de sous-réseau pour une route, cliquez sur le champ correspondant, entrez la nouvelle valeur et cliquez ensuite sur *Apply*.

Pour éditer le coût et l'interface d'une route, cliquez sur le lien *Advanced Options* pour cette route et entrez les nouvelles valeurs. Cliquez ensuite sur *OK*.

Pour supprimer une route existante, cochez la case *Delete ?* en regard de la route que vous désirez supprimer, puis cliquez sur *Apply*.

5.10.1. Créer une route IPv4

Pour créer une route IPv4, cliquez sur *Create new IPv4 Route…*. La page *Create new IPv4 Route* s'affiche :



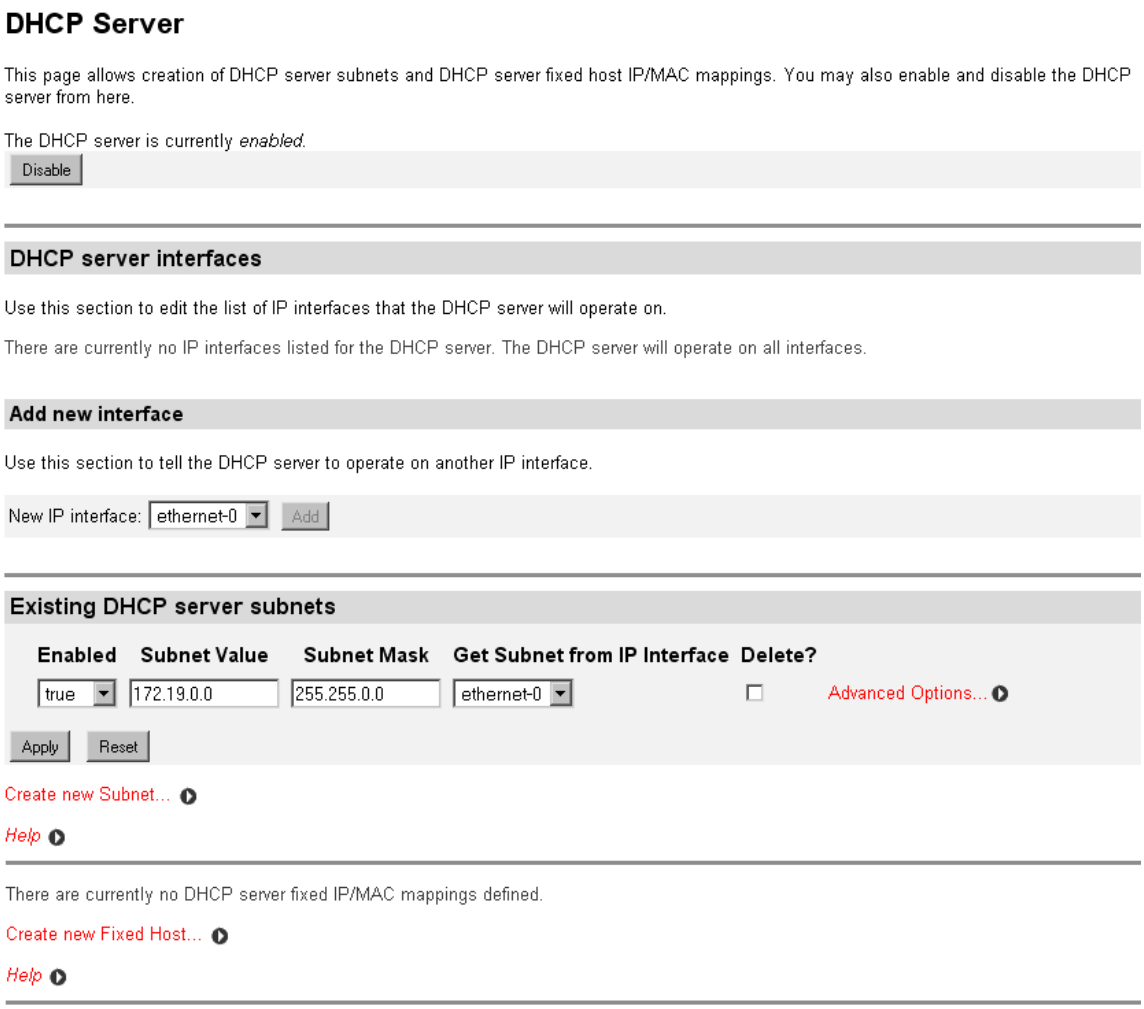
Complétez les champs avec les données nécessaires pour configurer la nouvelle route. Le bouton *Reset* vous permet de réinitialiser les valeurs. Lorsque vous avez terminé, cliquez sur *OK*. La page *Edit Routes* s'affiche. La liste contient maintenant les détails de la nouvelle route que vous avez créée.

5.11. Serveur DHCP – DHCP Server

DHCP vous permet d'assigner dynamiquement des adresses IP aux ordinateurs connectés à l'Ethernet de la Scarlet Box. La Scarlet Box permet de configurer plusieurs serveurs *DHCP* dans différents sous-réseaux. Habituellement, un seul serveur *DHCP* est nécessaire.

5.11.1. Configurer un serveur DHCP

Pour activer le serveur *DHCP*, ouvrez le menu *Configuration* et cliquez sur *DHCP server*. La page *DHCP server* s'affiche :

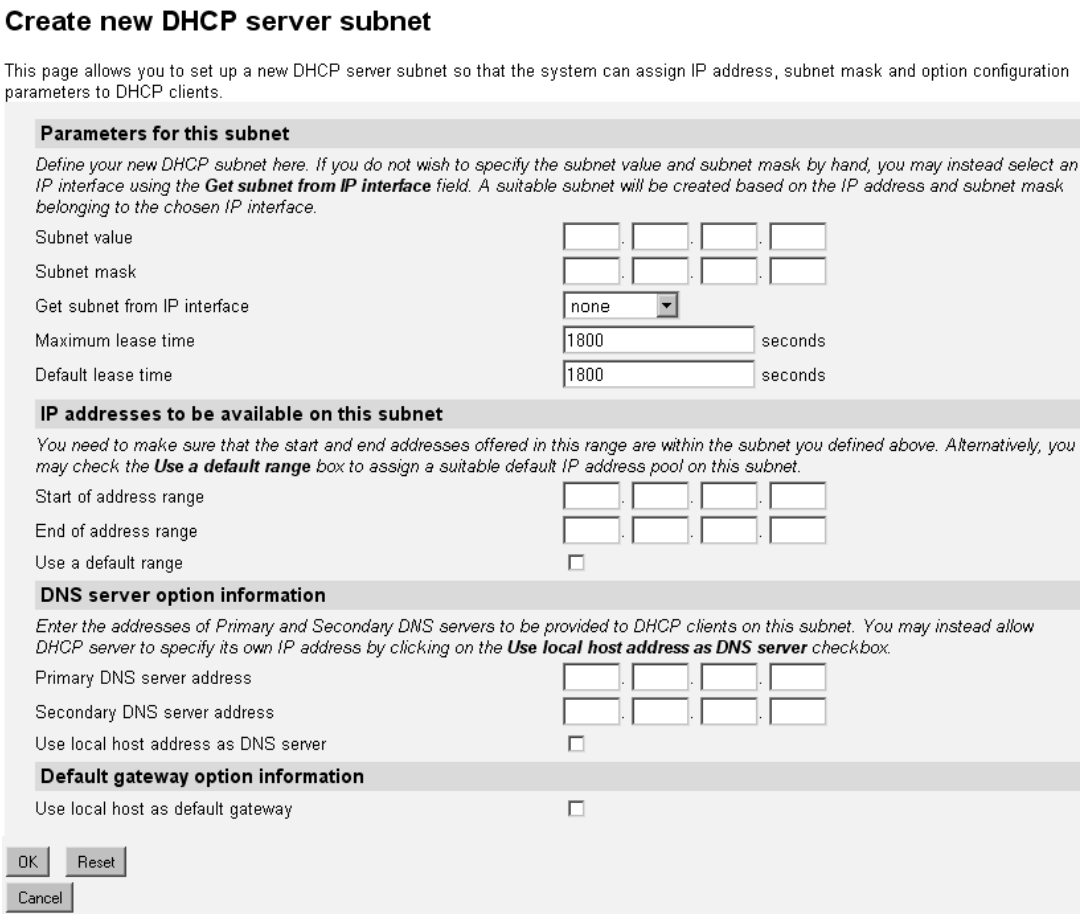

DHCP Server
This page allows creation of DHCP server subnets and DHCP server fixed host IP/MAC mappings. You may also enable and disable the DHCP server from here.
The DHCP server is currently enabled.
Disable
DHCP server interfaces
Use this section to edit the list of IP interfaces that the DHCP server will operate on.
There are currently no IP interfaces listed for the DHCP server. The DHCP server will operate on all interfaces.
Add new interface
Use this section to tell the DHCP server to operate on another IP interface.
New IP interface: ethernet-0
Add
Existing DHCP server subnets
Enabled
Subnet Value
Subnet Mask
Get Subnet from IP Interface
Delete?
true
172.19.0.0
255.255.0.0
ethernet-0
Advanced Options...
Apply
Reset
Create new Subnet...
Help
There are currently no DHCP server fixed IP/MAC mappings defined.
Create new Fixed Host...
Help

Cliquez sur le bouton *Enable*.

Au niveau *Add New Interface*, sélectionnez l'interface que vous désirez utiliser et cliquez sur *Add*. *Ethernet-0* est uniquement disponible à ce moment.

Après que vous ayez activé le serveur *DHCP* en cliquant sur le bouton *Enable*, vous devez définir des sous-réseaux pour le serveur *DHCP*.

Cliquez sur *Create new Subnet…*. La page *Create new DHCP server subnet* s'affiche :


Create new DHCP server subnet
This page allows you to set up a new DHCP server subnet so that the system can assign IP address, subnet mask and option configuration parameters to DHCP clients.
Parameters for this subnet
Define your new DHCP subnet here. If you do not wish to specify the subnet value and subnet mask by hand, you may instead select an IP interface using the Get subnet from IP interface field. A suitable subnet will be created based on the IP address and subnet mask belonging to the chosen IP interface.
Subnet value
Subnet mask
Get subnet from IP interface
none
Maximum lease time
1800
seconds
Default lease time
1800
seconds
IP addresses to be available on this subnet
You need to make sure that the start and end addresses offered in this range are within the subnet you defined above. Alternatively, you may check the Use a default range box to assign a suitable default IP address pool on this subnet.
Start of address range
End of address range
Use a default range
DNS server option information
Enter the addresses of Primary and Secondary DNS servers to be provided to DHCP clients on this subnet. You may instead allow DHCP server to specify its own IP address by clicking on the Use local host address as DNS server checkbox.
Primary DNS server address
Secondary DNS server address
Use local host address as DNS server
Default gateway option information
Use local host as default gateway
OK
Reset
Cancel

Cette page vous permet de :

- Choisir le sous-réseau du serveur *DHCP* manuelle **OU** utiliser le même sous-réseau que celui de l'interface IP en sélectionnant *ethernet-0*.

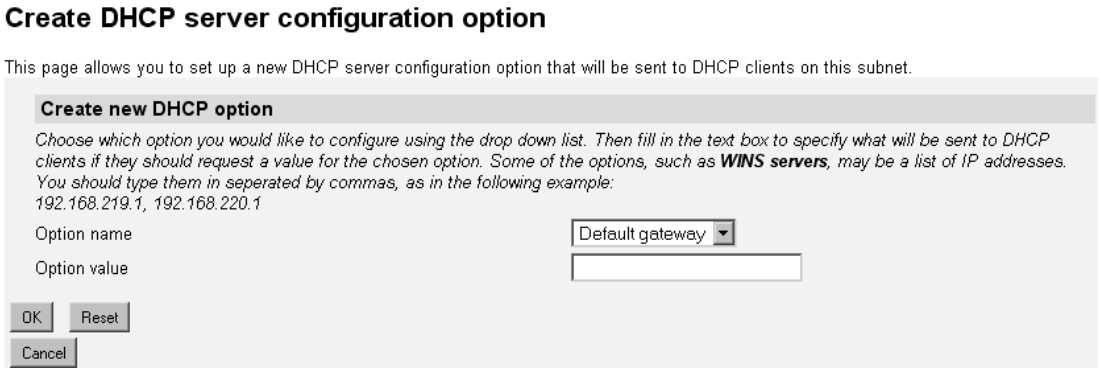
  Default lease time : si le client qui demande le bail ne précise pas de délai d'expiration, ce temps par défaut (en secondes) lui sera assigné (43200).

  Max lease time : le délai maximum (en secondes) qu'un sous-réseau peut assigner à un bail si le client qui réclame le bail ne précise pas le délai d'expiration (86400).
- Choisir l'intervalle *DHCP* d'adresses manuellement **OU** utiliser un intervalle par défaut de 253 adresses si vous choisissez *Use Default Range*.
- Configurer la Scarlet Box pour donner sa propre adresse IP comme serveur *DNS* **OU** choisir manuellement les adresses des serveurs *DNS* primaire et secondaire. Quand *Use Router as DNS Server* est sélectionné, le relais *DNS* est activé.
- Configurer la Scarlet Box pour donner sa propre adresse IP comme passerelle par défaut. Dans la plupart des situations, ceci est activé.

Dès que vous avez entré les détails de la nouvelle configuration pour votre serveur *DHCP*, cliquez sur *OK*. Vous reviendrez à la page *DHCP Server*, sur laquelle vous verrez que le nouveau sous-réseau *DHCP* a été ajouté. Pour supprimer un sous-réseau *DHCP*, cochez la case *Delete ?* en regard et cliquez sur *Apply*.

Pour accéder aux options avancées, cliquez sur le lien *Advanced Options…*. Cela vous permet d'éditer les valeurs déclarées quand le sous-réseau est créé. Ces valeurs font partie d'un ensemble de paramètres communiqués aux clients DHCP. En bas de la page, cliquez

sur le lien *Create new DHCP option*. La page *Create DHCP server configuration option* s'affiche :


Create DHCP server configuration option
This page allows you to set up a new DHCP server configuration option that will be sent to DHCP clients on this subnet.
Create new DHCP option
Choose which option you would like to configure using the drop down list. Then fill in the text box to specify what will be sent to DHCP clients if they should request a value for the chosen option. Some of the options, such as WINS servers, may be a list of IP addresses. You should type them in seperated by commas, as in the following example:
192.168.219.1, 192.168.220.1
Option name
Default gateway
Option value
OK
Reset
Cancel

Cliquez sur la liste déroulante *Option name* pour choisir l'option à éditer. Entrez alors une valeur adéquate dans la case *Option value*. Cliquez ensuite sur le bouton *OK*.

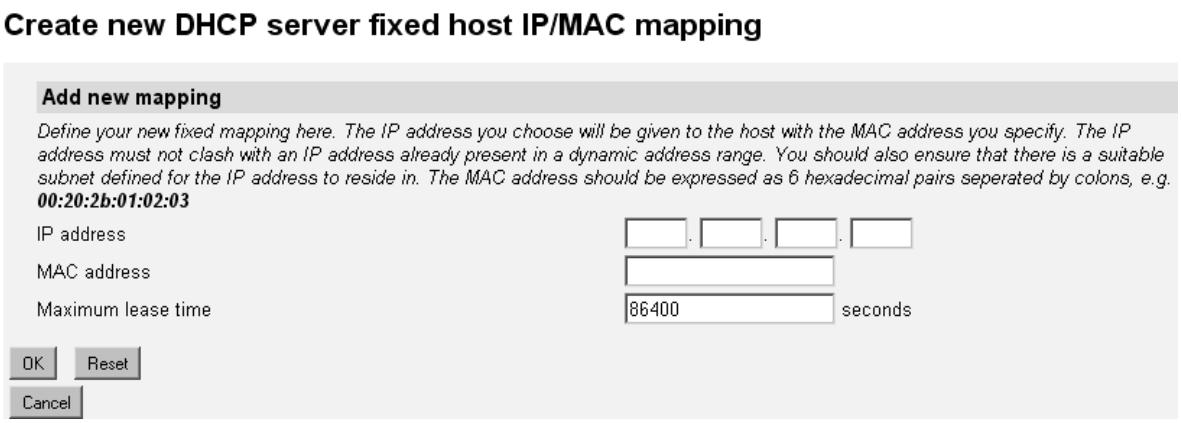
La page *Edit DHCP server subnet* s'affiche et les détails de la nouvelle option sont présents sous le sous-titre *Additional option information*. Pour supprimer une option existante, cochez la case *Delete ?* en regard de l'option à supprimer et cliquez sur *OK*.

Ouvrez le menu *Configuration* et cliquez sur *Save config* pour enregistrer les nouveaux paramètres dans la mémoire de la Scarlet Box.

5.11.2. Créer un hôte fixe – Create fixed host

Un hôte fixe est une adresse IP réservée pour un ordinateur dans le serveur DHCP. Lorsque cet ordinateur demande un bail, cette adresse IP lui est automatiquement affectée, et à aucun autre ordinateur.

Pour créer un hôte fixe, cliquez sur *Create new Fixed Host…*. La page *Create new DHCP server fixed host IP/MAX mapping* s'affiche:


Create new DHCP server fixed host IP/MAC mapping
Add new mapping
Define your new fixed mapping here. The IP address you choose will be given to the host with the MAC address you specify. The IP address must not clash with an IP address already present in a dynamic address range. You should also ensure that there is a suitable subnet defined for the IP address to reside in. The MAC address should be expressed as 6 hexadecimal pairs seperated by colons, e.g. 00:20:2b:01:02:03
IP address
MAC address
Maximum lease time
86400
seconds
OK
Reset
Cancel

Procédez comme suit:

- Introduisez l'adresse IP qui sera associée avec l'adresse MAC suivante
- Entrez l'adresse MAC (adresse physique de la carte réseau) à laquelle vous souhaitez associer la précédente adresse IP, ainsi que le délai maximum pour le bail

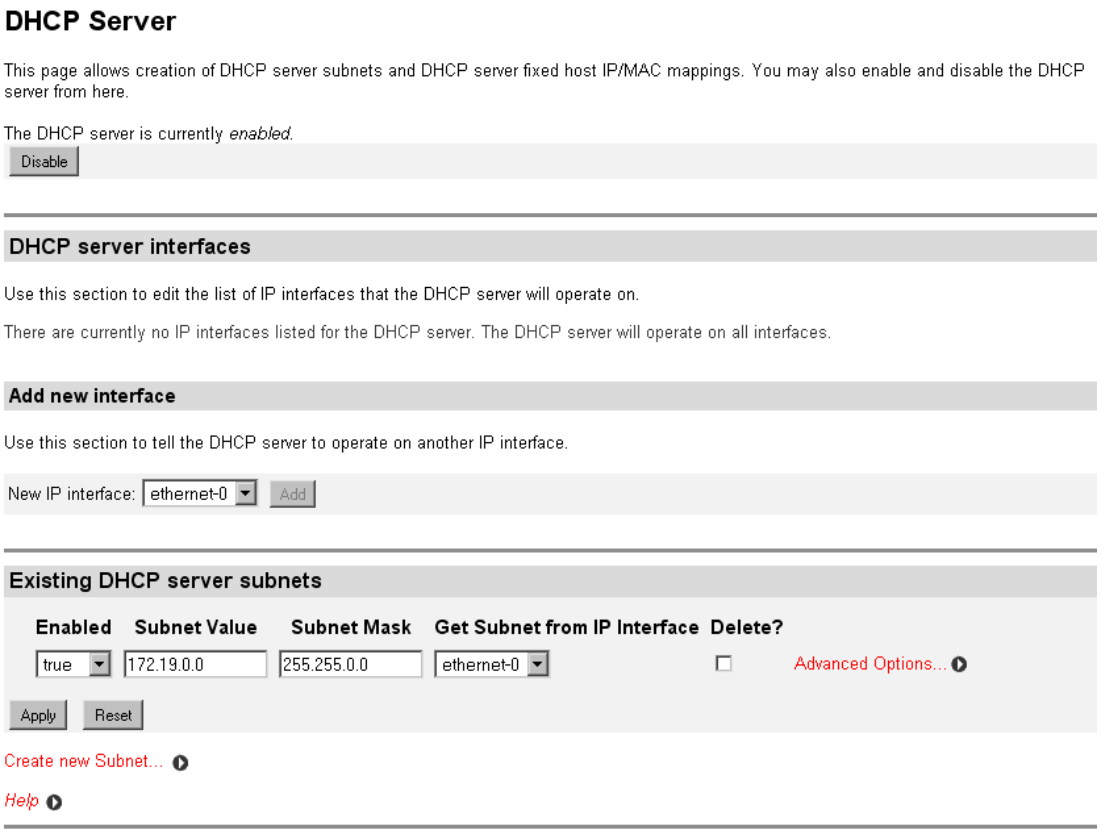
- Cliquez sur *OK*. La page *DHCP Server* s'affiche avec les détails du nouvel hôte fixe sous le sous-titre *Existing DHCP fixed IP/MAC mappings*.

Pour éditer une association, cliquez sur l'adresse IP, l'adresse MAC ou le délai de bail que vous souhaitez modifier, entrez les nouvelles valeurs et cliquez sur *Apply*. Pour supprimer une association, cochez la case *Delete ?* en regard de l'association et cliquez sur *Apply*.

Ouvrez le menu *Configuration* et cliquez sur *Save config* pour enregistrer les modifications dans la mémoire de votre Scarlet Box.

5.11.3. Désactiver le serveur DHCP

Pour désactiver le serveur DHCP, ouvrez le menu *Configuration* et cliquez sur *DHCP server*. La page *DHCP Server* s'affiche :

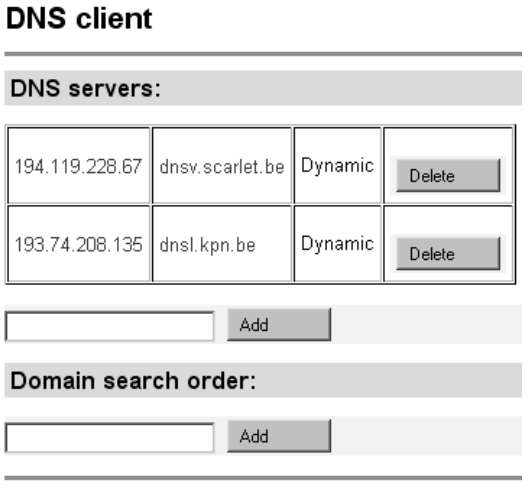

DHCP Server
This page allows creation of DHCP server subnets and DHCP server fixed host IP/MAC mappings. You may also enable and disable the DHCP server from here.
The DHCP server is currently enabled.
Disable
DHCP server interfaces
Use this section to edit the list of IP interfaces that the DHCP server will operate on.
There are currently no IP interfaces listed for the DHCP server. The DHCP server will operate on all interfaces.
Add new interface
Use this section to tell the DHCP server to operate on another IP interface.
New IP interface: ethernet-0 Add
Existing DHCP server subnets
Enabled Subnet Value Subnet Mask Get Subnet from IP Interface Delete?
true 172.19.0.0 255.255.0.0 ethernet-0 Advanced Options...
Apply Reset
Create new Subnet...
Help

Cliquez sur le bouton *Disable*. Le serveur DHCP est alors désactivé.

Ouvrez le menu *Configuration* et cliquez sur *Save config* pour enregistrer les modifications dans la mémoire de votre Scarlet Box.

5.12. Configurer le client DNS

Pour configurer manuellement le relais DNS (*DNS relay)*, ouvrez le menu *Configuration* et cliquez sur *DNS relay*. La page *DNS Relay* s'affiche :



5.12.1. Configurer des serveurs DNS

- Entrez l'adresse IP d'un serveur DNS dans la première case libre de la section *DNS servers.*
- Cliquez sur le bouton *Add*. L'adresse IP du nouveau serveur DNS apparaît alors dans la liste des serveurs DNS. Vous pouvez ajouter jusque 3 adresses IP de serveurs DNS. Chaque adresse IP de la liste possède un bouton *Delete* qui lui est associé. Cliquez sur le bouton *Delete* pour supprimer une adresse IP de la liste.

Note : vous pouvez trouver les serveurs DNS de Scarlet à l'adresse http://www.scarlet.be/fr/assistance/.

5.12.2. Configurer les domaines DNS à explorer

- Entrez le nom d'un domaine à explorer dans la première case libre de la section *Domain search order*.
- Cliquez sur le bouton *Add*. Le nouveau nom de domaine apparaît alors dans la liste des domaines à explorer. Vous pouvez ajouter jusqu'à 6 domaines à explorer. Chaque nom possède un bouton *Delete* qui lui est associé. Cliquez sur le bouton *Delete* pour supprimer un nom de la liste.

Note : pour utiliser le réseau Scarlet, laissez la liste des noms de domaines à explorer vide.

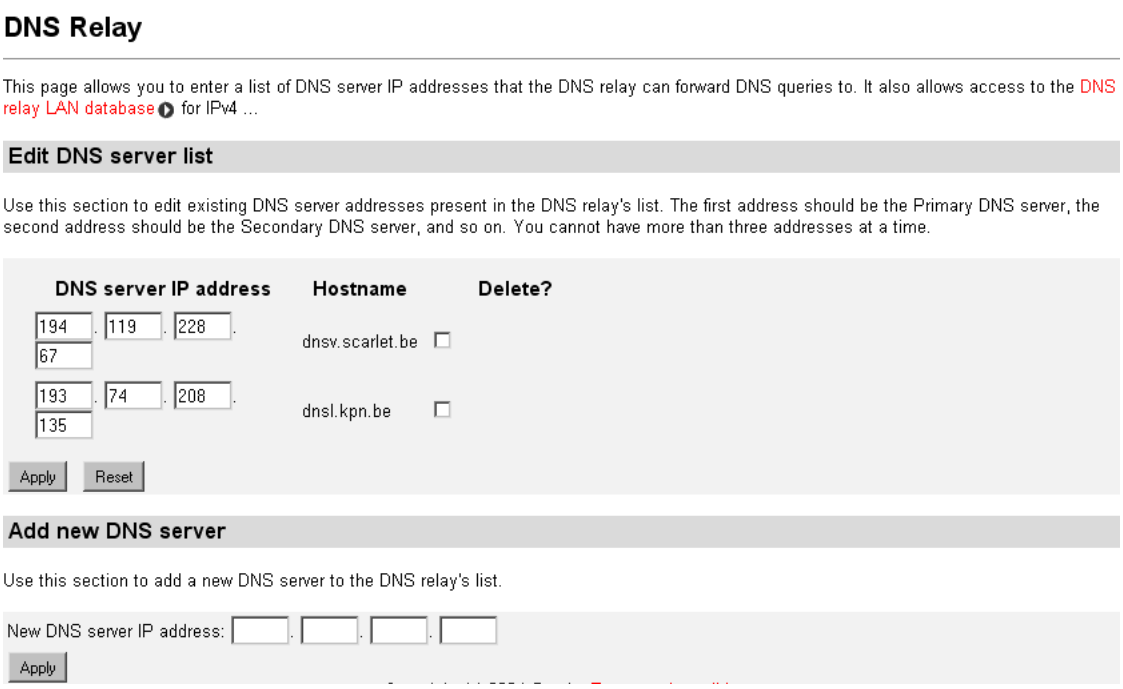
5.13. Configurer le relais DNS

Le relais DNS vous permet d'adresser les requêtes DNS de vos ordinateurs à la Scarlet Box au lieu des serveurs DNS de votre fournisseur d'accès. La Scarlet Box se charge alors de relayer les requêtes vers les serveurs DNS spécifiés.

Les serveurs DNS peuvent être découverts automatiquement grâce à DHCP sur l'interface externe WAN **OU** configurés manuellement.

5.13.1. Configurer manuellement le relais DNS

Pour configurer manuellement le relais DNS, ouvrez le menu *Configuration* et cliquez sur *DNS relay*. La page *DNS Relay* s'affiche :


DNS Relay
This page allows you to enter a list of DNS server IP addresses that the DNS relay can forward DNS queries to. It also allows access to the DNS relay LAN database for IPv4 ...
Edit DNS server list
Use this section to edit existing DNS server addresses present in the DNS relay's list. The first address should be the Primary DNS server, the second address should be the Secondary DNS server, and so on. You cannot have more than three addresses at a time.
DNS server IP address
Hostname
Delete?
194 . 119 . 228 . 67
dnsv.scarlet.be
193 . 74 . 208 . 135
dnsl.kpn.be
Apply
Reset
Add new DNS server
Use this section to add a new DNS server to the DNS relay's list.
New DNS server IP address: . . .
Apply

Entrez les adresses IP des serveurs DNS dans la section *Add new DNS server*. Pour chaque serveur ajouté, cliquez sur *Apply*. Vous pourrez alors voir les adresses IP ajoutées dans la section. Pour éditer une adresse IP, corrigez sa valeur dans la section Edit *DNS server list* et cliquez sur le bouton *Apply*.
Pour supprimer une adresse IP, cochez la case *Delete ?* en regard de l'adresse et cliquez sur *Apply*.
Le bouton *Reset* vous permet de mettre toutes les valeurs à blanc.

Lorsque vous avez terminé de configurer les relais DNS, ouvrez le menu *Configuration* et cliquez sur *Save config* pour enregistrer les nouveaux paramètres dans la mémoire de votre Scarlet Box.

Note : vous devez configurer l'adresse IP de votre Scarlet Box comme serveur DNS pour les ordinateurs de votre réseau, ou configurer le serveur DHCP de votre Scarlet Box pour qu'il attribue ce serveur automatiquement, à l'aide de l'option *Use Router as DNS Server* (voir point 5.11.1)

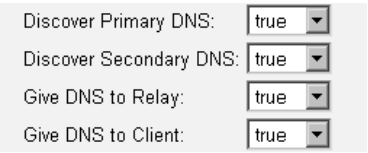
5.13.2. Découvrir automatiquement les adresses DNS relais

Pour configurer la découverte automatique des adresses DNS relais, vous devez avoir configuré une connexion WAN. Voyez la section 5.6 pour configurer une connexion WAN.

Aussi bien pour les connexions PPPoA que PPPoE, la Scarlet Box peut découvrir les adresses DNS automatiquement. Le fournisseur d'accès doit fournir les adresses des serveurs DNS via DHCP. Dans ce cas, il n'est pas nécessaire de configurer le relais DNS manuellement. Ouvrez le menu *Configuration* et cliquez sur *WAN Connections*. Les connexions WAN définies sont affichées. Editez la connexion WAN concernée en cliquant sur le lien *Edit*. La page *WAN connection* s'affiche.

Pour une connexion PPPoA, cliquez sur l'onglet *PPP*. Pour une connexion PPPoE, cliquez sur l'onglet *PPPoE*.

Assurez-vous que les options suivantes sont bien positionnées sur *true* si vous désirez que la Scarlet Box découvre et passe les adresses DNS automatiquement.

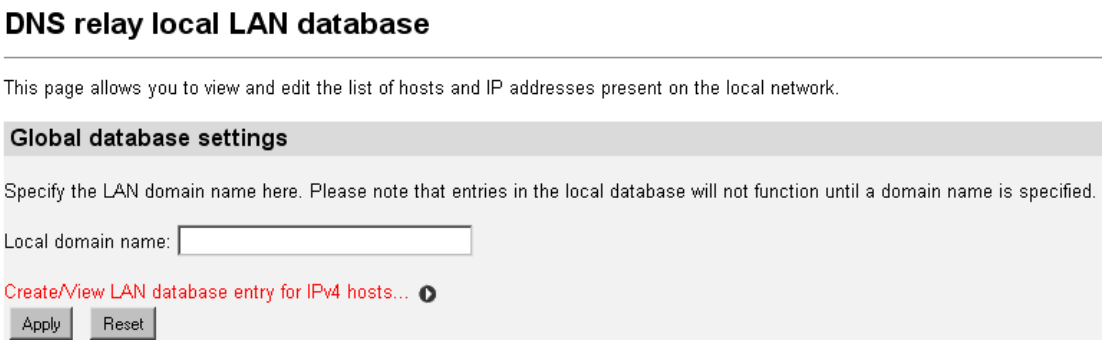


vous avez terminé de configurer les relais DNS pour la connexion WAN, cliquez sur *Apply*. Ouvrez le menu *Configuration* et cliquez sur *Save config*, afin d'enregistrer vos nouveaux paramètres dans la mémoire de la Scarlet Box.

Note : vous devez configurer l'adresse IP de votre Scarlet Box comme serveur DNS pour les ordinateurs de votre réseau, ou configurer le serveur DHCP de votre Scarlet Box pour qu'il attribue ce serveur automatiquement, à l'aide de l'option *Use Router as DNS Server* (voir point 5.11.1)

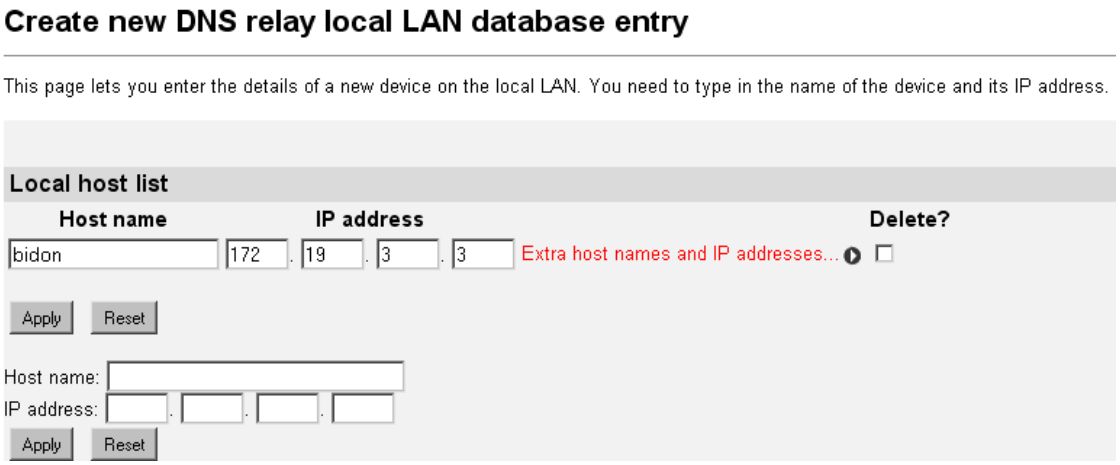
5.13.3. Configurer la base de données DNS du réseau local

La base de données DNS du réseau local vous permet d'associer des noms d'hôtes locaux avec des adresses IP dans le DNS de la Scarlet Box, qui fait alors office de serveur DNS local. Pour configurer la base de données, cliquez sur *DNS relay LAN database*. La page *DNS relay local LAN database* s'affiche :


DNS relay local LAN database
This page allows you to view and edit the list of hosts and IP addresses present on the local network.
Global database settings
Specify the LAN domain name here. Please note that entries in the local database will not function until a domain name is specified.
Local domain name:
Create/View LAN database entry for IPv4 hosts...
Apply
Reset

Pour configurer un nom de domaine local, entrez-le dans la case *Local domain name*. Ceci permet au relais DNS de la Scarlet Box de déterminer si une requête porte sur un nom d'hôte local ou pas.

Pour créer un nouveau nom d'hôte local, cliquez sur *Create/View LAN database entry for IPv4 hosts…*. La page *Create new DNS relay local LAN database entry* s'affiche:



Entrez le nom d'hôte et l'adresse IP dans les champs correspondant et cliquez sur *Apply*. La page *DNS relay local LAN database* est alors rechargée. Pour visualiser les hôtes locaux, cliquez sur *Create/View LAN database entry for IPv4 hosts*.

Pour modifier un enregistrement existant, modifiez les valeurs adéquates et cliquez sur *Apply*. Pour supprimer un enregistrement, cochez la case *Delete ?* en regard de l'enregistrement à supprimer et cliquez sur *Apply*.

Pour configurer un alias pour un hôte local, cliquez sur le lien *Extra host names and IP adresses…* en regard de l'hôte à configurer. La page qui s'affiche vous permet de :

- Créer un nouveau nom d'hôte et/ou un alias de l'adresse IP. Entrez le nouveau nom et/ou adresse IP et cliquez sur *Apply*.
- Modifier un nom d'hôte et/ou un alias de l'adresse IP. Entrez le nouveau nom et/ou adresse IP et cliquez sur *Apply*.
- Supprimer un nom d'hôte ou un alias d'adresse IP. Cochez la case *Delete ?* en regard de la donnée à supprimer et cliquez sur *Apply*.

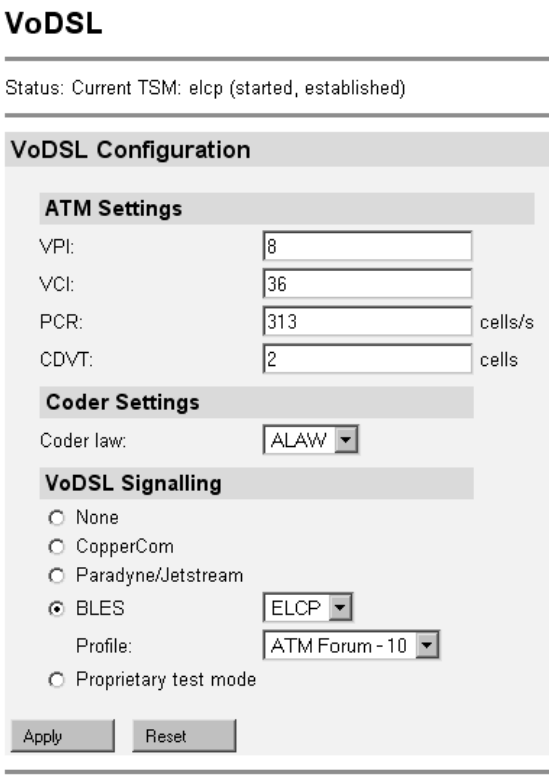
5.14. Configurer le service Voix sur DSL – Voice over DSL

La configuration de base du service voix sur DSL (VoDSL) de la Scarlet Box peut se faire via l'interface de configuration web. Les réglages pointus ne peuvent se faire qu'à travers l'interface telnet.

Important : le service VoDSL vous permet de profiter du service de téléphonie de Scarlet. Une mauvaise configuration de ce service peut vous empêcher d'émettre et/ou de recevoir des appels téléphoniques !

5.14.1. Paramètres de base du service Voix sur DSL

Pour configurer les paramètres de base du service voix sur DSL, ouvrez le menu *Configuration* et cliquez sur *VoDSL*. La page *VoDSL* s'affiche :



Vous pouvez ajuster la configuration pour le VoDSL. Les valeurs des paramètres doivent vous avoir été communiqué par votre fournisseur de service VoDSL.

Note : cette capture d'écran présente les valeurs utilisées par Scarlet sur son réseau de téléphonie utilisant la voix sur DSL.

VPI : *Virtual Path Identifier*, identifiant de chemin virtuel. Il s'agit d'un champ dans l'entête ATM qui permet d'identifier le chemin virtuel auquel un circuit appartient. Le VPI peut prendre toute valeur entre 0 et 4095. Pour Scarlet, la valeur à utiliser est 8.

VCI : *Virtual Channel Identifier*, identifiant de canal virtuel. Il s'agit d'un marqueur qui identifie le canal sur lequel une cellule voyage. Le VCI peut prendre toute valeur entre 1 et 65535. Pour Scarlet, la valeur à utiliser est 36.

Coder Law : *ALAW* est généralement utilisé en Europe, *ULAW* aux Etats-Unis.

None : aucune signalétique VoDSL configurée.

CopperCom : signalétique VoDSL propriétaire CopperCom

Paradyne/Jetstream : signalétique VoDSL propriétaire Paradyne/Jetstream

BLES : signalétique VoDSL BLES

ELCP : *ELCP* est un protocole standard qui définit le mécanisme selon lequel des messages basés sur V5.2 sont échangés entre la passerelle VoDSL et le terminal afin de supporter à la fois *POTS* (*Plain Old Telephone System*, la téléphonie classique) et la voix ISDN sur ATM.

CAS : *Channel Associated Signaling*, utilisé dans les schémas binaires où une partie de la bande passante est dédiée pour la signalétique dans chaque connexion

Profile : Sélectionnez *ITU-T (voice over AAL2)* ou *ATM-Forum (AF-voice traffic over ATM (VTOA))*. L'identifiant et la source du profile sont uniquement utilisés pour la signalétique BLES (pour CAS et ELCP). Pour les passerelles vocales disposant uniquement d'un mode ADPCM (pour toutes les valeurs entre 0 et 15), le profile atmforum spécial 13 est utilisé.

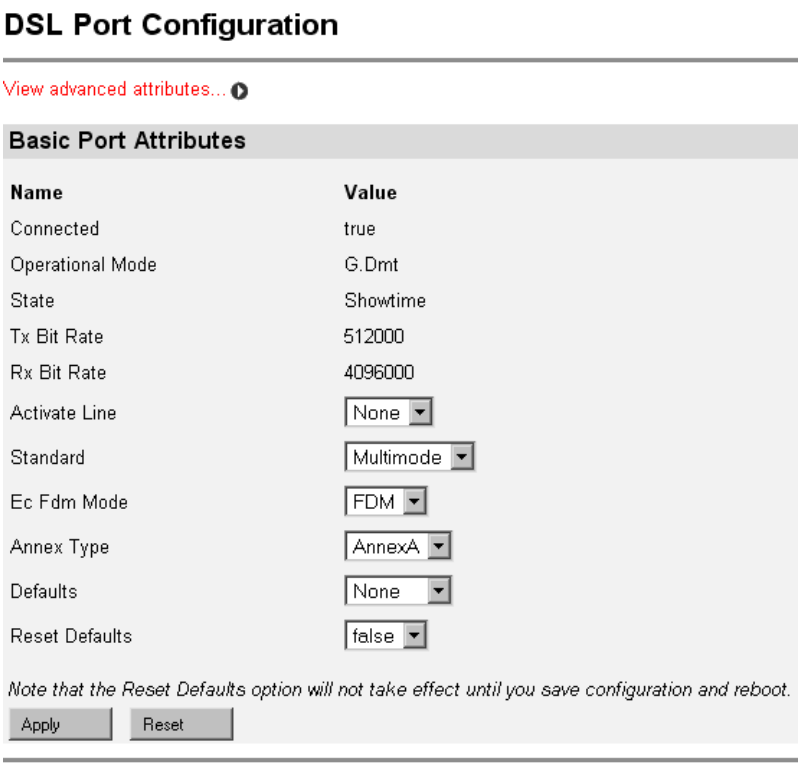
Proprietary test mode :
Ce mode active les fonctionnalités PBX internes afin de tester les ports vocaux.
Port vocal 1 : numéro 101.
Port vocal 2 : numéro 102.

Lorsque vous avez terminé de configurer le service VoDSL, cliquez sur *Apply*. Ouvrez le menu *Configuration* et cliquez sur *Save config*, afin d'enregistrer vos nouveaux paramètres dans la mémoire de la Scarlet Box.

5.15. Ligne DSL – DSL Line

Le menu *DSL Port* vous permet de configurer des paramètres DSL spécifiques. Généralement, les valeurs par défaut sont suffisantes pour établir une bonne connexion DSL. Si vous souhaitez ajuster des valeurs ou effectuer de l'administration avancée, le menu *DSL port* vous fournit des informations utiles.

Ouvrez le menu *Configuration*, cliquez sur *Ports* puis sur *DSL*. La page *DSL Port Configuration* s'affiche :



Cette page vous fournit les informations suivantes :

Connected : détermine si votre ligne DSL est active (*true*) ou pas (*false*)

Operational Mode : le type de modulation utilisée pour établir la connexion.

State : fournit le statut de la ligne : *Handshake* (négociation), *Training* (contrôle de fiabilité) ou *Showtime* (ligne opérationnelle).

Tx Bit Rate : la vitesse d'envoi de votre ligne DSL

RX Bit Rate : la vitesse de réception de votre ligne DSL

Activate Line : *None* : le lien DSL ne sera pas activé
Abort : le lien DSL sera désactivé
Start : le lien DSL sera activé.

Whip : protocole propriétaire, désactivé par défaut.

Standard : *MultiMode* par défaut

Ec Fdm Mode : *FDM* par défaut

Annex Type : affiche le type d'annexe que vous avez

Default : aucun par défaut

Reset default : *false* par défaut. Force une réinitialisation des paramètres lorsqu'il est positionné sur *true*.

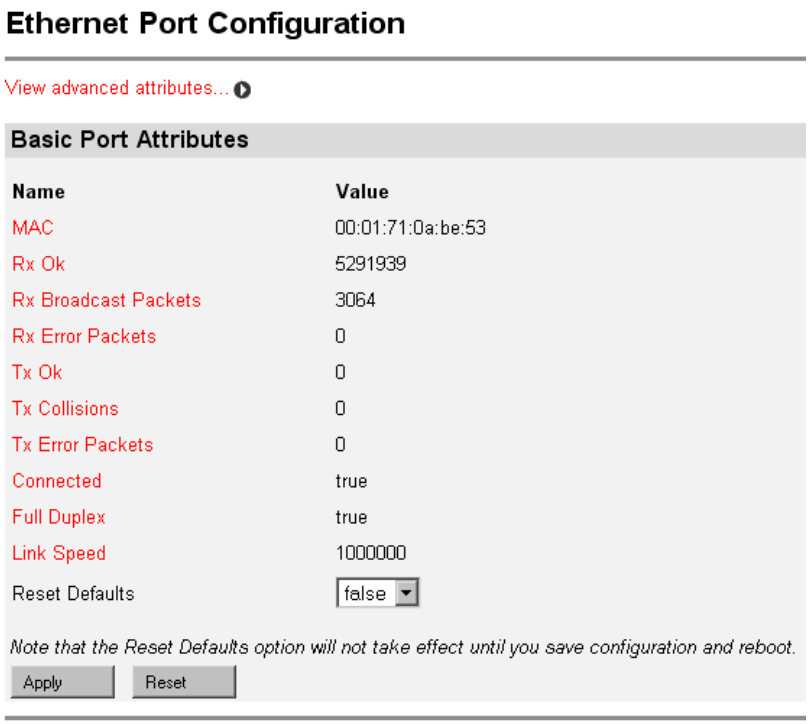
Cliquez sur R*eset* pour retrouver les paramètres précédents.

Lorsque vous avez terminé de modifier la configuration, cliquez sur *Apply*. N'oubliez pas d'enregistrer vos modifications : ouvrez le menu *Configuration* et cliquez sur *Save config* pour enregistrer vos nouveaux paramètres dans la mémoire de la Scarlet Box.

5.16. Ethernet

La page *Ethernet Port Configuration* vous fournit des informations utiles sur la connexion Ethernet de votre Scarlet Box.

Ouvrez le menu *Configuration*, cliquez sur *Ports* puis sur *Ethernet*. La page *Ethernet Port Configuration* s'affiche :



Cliquez sur une information pour obtenir de l'aide.